

Διπλωματική Εργασία
Νιέρης Ιωάννης
Επιβλέπων Καθηγητής: Τύρος Κωνσταντίνος

Το πρόβλημα discrepancy του Erdős

Τμήμα Μαθηματικών
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
Ιούνιος 2023

Τριμελής επιτροπή

Τύρος Κωνσταντίνος, Αναπληρωτής Καθηγητής, Τμήμα Μαθηματικών, ΕΚΠΑ

Δοδός Παντελής, Αναπληρωτής Καθηγητής, Τμήμα Μαθηματικών, ΕΚΠΑ

Μπαρμπάτης Γεράσιμος, Καθηγητής, Τμήμα Μαθηματικών, ΕΚΠΑ

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Κωνσταντίνο Τύρο για τον χρόνο που αφιέρωσε και την άριστη συνεργασία που είχαμε καθ' όλη την διάρκεια της διπλωματικής μου εργασίας.

Επίσης, θέλω να ευχαριστήσω τους κυρίους Παντελή Δοδό και Γεράσιμο Μπαρμπάτη για την συμμετοχή τους στην Τριμελή επιτροπή.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και την κοπέλα μου Μαρία για την αμέριστη στήριξη που μου παρέχουν όλα αυτά τα χρόνια.

Περίληψη

Στόχος της παρούσας διπλωματικής εργασίας είναι η παρουσίαση της απόδειξης του Terence Tao [5], πάνω στο ερώτημα του Erdős, για τον αν κάθε ακολουθία αριθμών $f(1), f(2), \dots$ που λαμβάνει τιμές στο $\{-1, +1\}$ έχει άπειρο discrepancy, δηλαδή αν η ποσότητα:

$$\sup_{n,d \in \mathbb{N}} \left| \sum_{j=0}^n f(jd) \right|$$

απειρίζεται. Η ίδια ερώτηση μπορεί να διατυπωθεί και για συναρτήσεις που παίρνουν τιμές πάνω στην σφαίρα ενός πραγματικού ή μιγαδικού χώρου Hilbert. Στις πρώτες δύο παραγράφους δίνονται κάποιοι βασικοί ορισμοί και προτάσεις, τα οποία θα μας φανούν χρήσιμα για την συνέχεια. Η απόδειξη χωρίζεται σε τρία μέρη:

- Στο πρώτο μέρος γίνεται η αντικατάσταση της συνάρτησης $f : \mathbb{N} \rightarrow \{-1, +1\}$ με μία συνάρτηση g η οποία είναι στοχαστική, πλήρως πολλαπλασιαστική (δηλαδή $g(nm) = g(n)g(m)$ για κάθε $n \in \mathbb{N}$) μέσω εργαλείων της ανάλυσης Fourier. Έτσι, πλέον θα έχουμε ένα πρόβλημα, το οποίο είναι ισοδύναμο με το αρχικό, αλλά πάνω σε πλήρως πολλαπλασιαστικές συναρτήσεις. Την διαδικασία αυτή την λαμβάνουμε από το Polymath5 project πάνω στο πρόβλημα του Erdős.
- Στο δεύτερο μέρος είναι η απόδειξη μιάς πρότασης (Van der Corput argument) η οποία θα φανεί χρήσιμη στο τρίτο μέρος και η απόδειξή της στηρίζεται πάνω σε ένα θεώρημα (logarithmically averaged version of the Elliott conjecture) που αποδείχθηκε από τον Terence Tao.
- Στο τρίτο μέρος αποδεικνύεται το ισοδύναμο θεώρημα πάνω στις πλήρως πολλαπλασιαστικές συναρτήσεις και τελικά ολοκληρώνεται και η απόδειξη πάνω στο ερώτημα του Erdős. Τα επιχειρήματα εδώ τα λαμβάνουμε από μία επέκταση της δουλειάς που προέκυψε από το Polymath5 project.

Περιεχόμενα

1	Στοιχεία αναλυτικής θεωρίας αριθμών	6
1.1	Η συνάρτηση Euler	6
1.2	Χαρακτήρες Dirichlet	9
1.3	Συνάρτηση L-Dirichlet	14
1.4	Περιοδικές αριθμητικές συναρτήσεις και αθροίσματα Gauss	14
1.5	Σειρές Dirichlet και γινόμενα Euler	20
1.6	Εκτιμήσεις Merten's	23
2	Στοιχεία ανάλυσης	25
2.1	Θεώρημα Prokhorov	25
2.2	Ταυτότητα Plancherel	27
3	Εισαγωγή στο πρόβλημα discrepancy του Erdős	29
3.1	Κεντρικό θεώρημα	29
3.2	Παραδείγματα	29
3.3	Σκιαγράφηση της απόδειξης του κεντρικού θεωρήματος	33
3.4	Συμβολισμοί	36
4	Fourier analytic reduction	37
5	Applying the Elliott – type conjecture	47
6	A generalised Borwein – Choi – Coons analysis	52
7	Βιβλιογραφία	78

1 Στοιχεία αναλυτικής θεωρίας αριθμών

Σε αυτή την παράγραφο θα αναφερθούμε σε ορισμούς και αποτελέσματα τα οποία αφορούν την αναλυτική θεωρία αριθμών, τα οποία είναι απαραίτητα για την κατανόηση και την απόδειξη του προβλήματος του Erdős. Πιο συγκεκριμένα, οι χαρακτήρες και οι σειρές Dirichlet, το γινόμενο Euler, οι εκτιμήσεις του Merten's, έχουν κεντρικό ρόλο στην διαδικασία της απόδειξης.

1.1 Η συνάρτηση Euler

Ορισμός 1.1.1. (Συνάρτηση Euler) Έστω n θετικός ακέραιος. Η συνάρτηση Euler $\phi(n)$ ορίζεται ως το πλήθος των θετικών ακεραίων, που δεν υπερβαίνουν τον n και είναι πρώτοι ως προς τον n . Έτσι είναι

$$\phi(n) = \sum_{1 \leq k \leq n: (k,n)=1} 1,$$

όπου $(k, n) = 1$ ο μέγιστος κοινός διαιρέτης του φυσικών n και k .

Θεώρημα 1.1.2. Έστω n θετικός ακέραιος με $n > 1$, τότε ισχύει ότι

$$\sum_{d|n} \phi(d) = n.$$

Απόδειξη. Θεωρούμε το σύνολο $S = \{1, 2, \dots, n\}$. Κατανέμουμε τα στοιχεία του S σε ξένα σύνολα ως εξής: Για κάθε διαιρέτη d του n , θέτουμε

$$A(d) = \{k : (k, n) = d, 1 \leq k \leq n\}.$$

Έτσι, το $A(d)$ αποτελείται από εκείνα τα στοιχεία του S , που έχουν με τον n μέγιστο κοινό διαιρέτη τον d . Τα σύνολα $A(d)$ είναι ξένα ανά δύο, ενώ η ένωσή τους είναι το σύνολο S . Κατά συνέπεια, αν $f(d)$ συμβολίζει το πλήθος των στοιχείων του $A(d)$, τότε θα είναι

$$\sum_{d|n} f(d) = n. \quad (1.1)$$

Παρατηρούμε ότι $(k, n) = d$ αν και μόνο αν $(k/d, n/d) = 1$. Επίσης, ισχύει ότι $0 < k \leq n$ αν και μόνο αν $0 < k/d \leq n/d$. Άρα, αν τεθεί $q = k/d$, τότε υπάρχει αμφιμονοσήμαντη αντιστοιχία μεταξύ των στοιχείων του $A(d)$ και των ακεραίων q με τις εξής ιδιότητες: $0 < q \leq n/d$ και $(q, n/d) = 1$. Το πλήθος αυτών των q είναι $\phi(n/d)$. Επομένως, $f(d) = \phi(n/d)$, συνεπώς η (1.1) γίνεται

$$\sum_{d|n} \phi(n/d) = n.$$

Όμως αυτή είναι ισοδύναμη με την $\sum_{d|n} \phi(d) = n$, διότι: όταν το d διατρέχει το σύνολο των διαιρετών του n , τότε το ίδιο συμβαίνει και για το n/d και αυτό ολοκληρώνει την απόδειξη. $\square$

Θεώρημα 1.1.3. (Πολλαπλασιαστικός τύπος για την $\phi(n)$) Για κάθε ακέραιο $n \geq 1$ ισχύει

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Για να αποδειχθεί το παραπάνω θεώρημα πρέπει πρώτα να ορίσουμε την συνάρτηση του Möbius $\mu(n)$ και να δώσουμε μία πρόταση που συνδέει τις συναρτήσεις $\phi(n)$ και $\mu(n)$.

Ορισμός 1.1.4. (Συνάρτηση Möbius) Η συνάρτηση Möbius $\mu(n)$ ορίζεται ως εξής: Για $n = 1$ έχουμε $\mu(1) = 1$. Αν $n > 1$ γράφουμε $n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$ (όπου p_i οι πρώτοι παράγοντες του n). Τότε ορίζουμε $\mu(n) = (-1)^k$, αν $a_1 = \dots = a_k = 1$, ενώ σε κάθε άλλη περίπτωση ορίζουμε $\mu(n) = 0$.

Επίσης, ισχύει η ακόλουθη πρόταση.

Πρόταση 1.1.5. (Σχέση $\phi(n)$ και $\mu(n)$) Έστω n ακέραιος με $n \geq 1$, τότε ισχύει

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Απόδειξη. 1.1.3 Αν $n = 1$ το γινόμενο είναι κενό και έτσι εννοείται ότι του δίνουμε την τιμή 1 και έχουμε το ζητούμενο.

Έστω $n > 1$ και έστω $p_1, \dots, p_r$ οι διαφορετικοί πρώτοι διαιρέτες του n . Το γινόμενο μπορεί να γραφεί ως εξής:

$$\prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) = 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \dots + \frac{(-1)^r}{p_1 \cdot \dots \cdot p_r}. \quad (1.2)$$

Πρέπει να παρατηρήσουμε ότι κάθε όρος στο δεξιό μέλος της (1.2) είναι της μορφής $+1/d$ ή $-1/d$. όπου d διαιρέτης του n , που είναι 1 ή γινόμενο από πρώτους παράγοντες. Ο αριθμητής $+1$ ή -1 είναι ακριβώς ίσος με $\mu(d)$ και επειδή $\mu(d) = 0$ όταν διαιρείται από το τετράγωνο οποιουδήποτε p_i είναι φανερό ότι το άθροισμα στην (1.2) είναι ίσο με

$$\sum_{d|n} \frac{\mu(d)}{d}. \quad (1.3)$$

Τελικά, από την σχέση (1.3) και την Πρόταση 1.1.5 έπεται το ζητούμενο. $\square$

Θεώρημα 1.1.6. (Ιδιότητες της $\phi(n)$) Η συνάρτηση Euler έχει τις εξής ιδιότητες:

- (i) $\phi(p^a) = p^a - p^{a-1}$, για κάθε πρώτο αριθμό p και κάθε ακέραιο $a \geq 1$.
- (ii) $\phi(mn) = \phi(m)\phi(n)(d/\phi(d))$, όπου $d = (m, n)$.
- (iii) $\phi(mn) = \phi(m)\phi(n)$, όταν $(m, n) = 1$.
- (iv) Αν $a|b$, τότε $\phi(a)|\phi(b)$.
- (v) Ο $\phi(n)$ είναι άρτιος για $n \geq 3$. Ακόμη, αν ο n έχει r διαφορετικούς περιττούς πρώτους παράγοντες, τότε $2^r | \phi(n)$.

Απόδειξη. (i) Προκύπτει άμεσα από το Θεώρημα 1.1.3 για $n = p^a$.

(ii) Από το Θεώρημα 1.1.3 γράφουμε

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Κατόπιν παρατηρούμε ότι κάθε πρώτος διαιρέτης του mn είναι διαιρέτης του m ή του n . Ακόμη, εκείνοι οι πρώτοι που διαιρούν και τον m και τον n είναι διαιρέτες και του (m, n) . Επομένως,

$$\frac{\phi(mn)}{mn} = \prod_{p|mn} \left(1 - \frac{1}{p}\right) = \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|(m,n)} \left(1 - \frac{1}{p}\right)} = \frac{\frac{\phi(m)}{m} \frac{\phi(n)}{n}}{\frac{\phi(d)}{d}},$$

όπου προκύπτει το ζητούμενο.

(iii) Είναι ειδική περίπτωση του (ii).

(iv) Επειδή $a|b$, θα είναι $b = ac$, όπου c ακέραιος με $1 \leq c \leq b$. Αν $c = b$, τότε $a = 1$ άρα έχουμε το ζητούμενο. Έστω $c < b$. Από το (ii) έχουμε

$$\phi(b) = \phi(ac) = \phi(a)\phi(c) \frac{d}{\phi(d)} = d\phi(a) \frac{\phi(c)}{\phi(d)}, \quad (1.4)$$

όπου $d = (a, c)$. Το αποτέλεσμα έπεται με επαγωγή στο b . Για $b = 1$ ισχύει προφανώς. Ας υποθεθεί ότι ισχύει για όλους τους ακέραιους οι οποίοι είναι γνήσια μικρότεροι του b . Τότε, ισχύει για τον c , οπότε θα είναι $\phi(d)|\phi(c)$, διότι $d|c$. Επομένως, το δεξιό μέλος της (1.4) είναι πολλαπλάσιο του $\phi(a)$, που σημαίνει ότι $\phi(a)|\phi(b)$ και αυτό ολοκληρώνει την απόδειξη.

(v) Αν $n = 2^a$, όπου a είναι ακέραιος με $a \geq 2$, τότε από το (i) έχουμε ότι $\phi(n)$ είναι άρτιος. Αν ο n έχει έναν τουλάχιστον περιττό πρώτο παράγοντα, τότε γράφουμε

$$\phi(n) = n \prod_{p|n} \frac{p-1}{p} = \frac{n}{\prod_{p|n} p} \prod_{p|n} (p-1) = c(n) \prod_{p|n} (p-1),$$

όπου ο $c(n)$ είναι ακέραιος. Το γινόμενο που πολλαπλασιάζει τον $c(n)$ είναι άρτιος αριθμός, οπότε ο $\phi(n)$ είναι άρτιος. Ακόμη, κάθε περιττός πρώτος p συνεισφέρει έναν παράγοντα 2 σε αυτό το γινόμενο $\prod_{p|n} (p-1)$. Άρα $2^r | \phi(n)$, όταν ο n έχει r διαφορετικούς περιττούς πρώτους παράγοντες. $\square$

1.2 Χαρακτήρες Dirichlet

Ορισμός 1.2.1. (Χαρακτήρας Dirichlet) Έστω q θετικός ακέραιος. Χαρακτήρας Dirichlet modulo q είναι μια συνάρτηση $x : \mathbb{N} \rightarrow \mathbb{C}$, η οποία ικανοποιεί τα ακόλουθα:

(i) $x(mn) = x(m)x(n)$, για κάθε $m, n \in \mathbb{N}$.

(ii) $x(m) \begin{cases} \neq 0 & , \text{ αν } (m, q) = 1 \\ = 0 & , \text{ αν } (m, q) > 1. \end{cases}$

(iii) $x(m + q) = x(m)$, για κάθε $m \in \mathbb{N}$.

Ορισμός 1.2.2. (Πρωταρχικός χαρακτήρας Dirichlet) Πρωταρχικός χαρακτήρας Dirichlet modulo q είναι η πιο απλή μορφή χαρακτήρα Dirichlet κατά την οποία:

$$x(m) = \begin{cases} 1 & , \text{ αν } (m, q) = 1 \\ 0 & , \text{ αν } (m, q) > 1. \end{cases}$$

Παρατηρήσεις 1.2.3. Έστω x χαρακτήρας Dirichlet modulo q . Τότε έχουμε τα παρακάτω:

(a) Εφόσον $(1, q) = 1$, από το (ii) του ορισμού 1.2.1 ισχύει ότι $x(1) \neq 0$. Συνεπώς,

$$x(1) \cdot x(1) = x(1 \cdot 1) = x(1) \Rightarrow x(1) = 1.$$

(b) Η ιδιότητα (iii) είναι ισοδύναμη με το εξής:

$$\text{Αν } m \equiv n \pmod{q}, \text{ τότε } x(m) = x(n).$$

(c) Από την ιδιότητα (i) προκύπτει άμεσα ότι για κάθε $n \in \mathbb{N}$ έχουμε ότι:

$$x(m^n) = (x(m))^n.$$

(d) Σύμφωνα με το θεώρημα Euler, για κάθε $(m, q) = 1$, ισχύει ότι $m^{\phi(q)} \equiv 1 \pmod{q}$.

Ειδικότερα,

$$(x(m))^{\phi(q)} = x(m^{\phi(q)}) = x(1) = 1.$$

Επομένως, οι μη-μηδενικές τιμές που παίρνει ένας χαρακτήρας Dirichlet είναι οι $\phi(q)$ -ρίζες της μονάδας.

Δηλαδή, ισχύει ότι:

$$x(m) = \begin{cases} \zeta_r^{\phi(q)} & , \text{ αν } (m, q) = 1 \\ 0 & , \text{ αν } (m, q) > 1, \end{cases}$$

όπου το r εξαρτάται από τα m, x με $r \in \{1, \dots, \phi(q)\}$ και $\zeta_r^{\phi(q)}$ μία $\phi(q)$ -ρίζα της μονάδας.

(e) Οι χαρακτήρες *Dirichlet modulo* q είναι πεπερασμένοι το πλήθος.

Πράγματι, υπάρχουν ακριβώς $\phi(q)$ φυσικοί αριθμοί που δέχονται μη μηδενικές τιμές και υπάρχουν $\phi(q)$ τιμές που μπορεί να πάρει ο καθένας, δηλαδή υπάρχουν το πολύ $(\phi(q))^{\phi(q)}$ χαρακτήρες *Dirichlet modulo* q .

Πρόταση 1.2.4. (Πλήθος χαρακτήρων *Dirichlet modulo* q) Έστω $q \in \mathbb{N}$. Τότε, υπάρχουν ακριβώς $\phi(q)$ το πλήθος χαρακτήρες *Dirichlet*.

Επιπλέον, για κάθε ακέραιο a με $(a, q) = 1$ και $a \not\equiv 1 \pmod{q}$, υπάρχει χαρακτήρας *Dirichlet* τέτοιος ώστε $x(a) \neq 1$.

Αρχικά, θα χρειαστούμε το παρακάτω λήμμα, η απόδειξη του οποίου δίνεται στο [4] σελίδα 176.

Λήμμα. Έστω q θετικός ακέραιος. Τότε, υπάρχουν θετικοί ακέραιοι $q_1, \dots, q_r$ οι οποίοι είναι σχετικά πρώτοι ως προς το q με τάξεις $h_1, \dots, h_r$ modulo q αντίστοιχα (δηλαδή οι θετικοί ακέραιοι h_i είναι οι ελάχιστοι για τους οποίους ισχύει $g_i^{h_i} \equiv 1 \pmod{q}$), με την εξής ιδιότητα:

Για κάθε ακέραιο n με $(n, q) = 1$, υπάρχουν μοναδικοί ακέραιοι n_i με $0 \leq n_i < h_i$, τέτοιοι ώστε $n \equiv \prod_{i=1}^r g_i^{n_i} \pmod{q}$. Ειδικότερα, έχουμε ότι $\prod_{i=1}^r h_i = \phi(q)$.

Απόδειξη. Έστω $g_1, \dots, g_r$ και $h_1, \dots, h_r$ όπως στο Λήμμα και έστω $\omega_j = e^{2\pi i/h_j}$, για $j = 1, 2, \dots, r$.

Άρα, ω_j^ν , με $\nu = 0, 1, \dots, h_j$, είναι οι διαφορετικές h_j -οστές ρίζες της μονάδας. Ισχυριζόμαστε ότι υπάρχει ένα προς ένα σχέση μεταξύ των ακολουθιών

$$\nu = (\nu_1, \dots, \nu_r), 0 \leq \nu_i < h_i \quad (1.5)$$

και των χαρακτήρων modulo q .

Αρχικά, έστω x ένας χαρακτήρας *Dirichlet modulo* q . Εξ'ορισμού $x(n) = 0$ όταν $(n, q) > 1$, και για ακέραιο n με $(n, q) = 1$, από το Λήμμα 1, έχουμε ότι $n \equiv \prod_{i=1}^r g_i^{\mu_i} \pmod{q}$, για μοναδικά $\mu_1, \dots, \mu_r$ με $0 \leq \mu_i < h_i$. Λόγω περιοδικότητας και πλήρους πολλαπλασιαστικότητας του χαρακτήρα, έχουμε την σχέση

$$x(n) = x\left(\prod_{i=1}^r g_i^{\mu_i}\right) = \prod_{i=1}^r x(g_i)^{\mu_i}, \quad (1.6)$$

για $n \equiv \prod_{i=1}^r g_i^{\mu_i}$. Άρα, ο χαρακτήρας καθορίζεται από τις τιμές του στους γεννήτορες g_i . Αφού, τα g_i έχουν τάξη h_i έχουμε

$$x(g_i)^{h_i} = x(g_i^{h_i}) = x(1) = 1,$$

και άρα το $x(g_i)$ αποτελεί h_i -οστή ρίζα της μονάδας.

Επιπλέον,

$$x(g_i) = \omega_i^{\nu_i}, \quad (1.7)$$

για μοναδικό $\nu = (\nu_1, \dots, \nu_r)$ όπως στη σχέση (1.5).

Αντίστροφα, έστω $\nu = (\nu_1, \dots, \nu_r)$. Ορίζουμε συνάρτηση $x : \mathbb{N} \rightarrow \mathbb{C}$ θέτοντας $x = x_\nu$ με $x(n) = 0$ για $(n, q) > 1$, και ορίζουμε $x(n)$ όπως στις σχέσεις (1.6) και (1.7) διαφορετικά. Εξ'ορισμού αυτής, έχουμε ότι η συνάρτηση x είναι q -περιοδική, είναι μηδενική για τους ακέραιους που δεν είναι πρώτοι ως προς το q και εύκολα προκύπτει ότι είναι και πλήρως πολλαπλασιαστική. Δηλαδή, είναι χαρακτήρας Dirichlet modulo q .

Έχουμε δείξει την ένα προς ένα αντιστοιχία και από το Λήμμα γνωρίζουμε ότι $h_1 \cdot \dots \cdot h_r = \phi(q)$, δηλαδή υπάρχουν ακριβώς $\phi(q)$ χαρακτήρες Dirichlet modulo q και η πρόταση έχει αποδειχθεί.

Για το δεύτερο μέρος της απόδειξης, έστω ακέραιος a με $(a, q) = 1$ και $a \not\equiv 1 \pmod{q}$. Από το Λήμμα, έχουμε ότι $a \equiv \prod_{i=1}^r g_i^{\mu_i} \pmod{q}$ για κατάλληλους εκθέτες της μορφής (1.5).

Εφόσον, $a \not\equiv 1 \pmod{q}$, τουλάχιστον ένας εκθέτης μ_i πρέπει να είναι μη μηδενικός. Χωρίς βλάβη της γενικότητας, θεωρούμε $\mu_1 \neq 0$. Ορίζουμε τον χαρακτήρα x με $x(g_1) = \omega_1$ και $x(g_i) = 1$ για $i \in \{2, \dots, r\}$. Τότε,

$$x(a) = x(g_1^{\mu_1}) = x(g_1)^{\mu_1} = \exp\left\{\frac{2\pi i \mu_1}{h_1}\right\} \neq 1,$$

αφού $0 < \mu_1 < h_1$. □

Παράδειγμα 1.2.5. Έστω ότι η περίοδος του χαρακτήρα Dirichlet είναι $q = 5$. Τότε, $\phi(5) = 4$ και άρα παίρνουμε τις 4-ρίζες της μονάδας, οι οποίες είναι: $1, -1, i, -i$. Σύμφωνα με την Πρόταση 1.2.4 υπάρχουν 4 χαρακτήρες Dirichlet modulo 5, έστω x_1, x_2, x_3, x_4 , και οι μη μηδενικές τιμές που παίρνουν είναι:

$$\begin{aligned} x_1(1) &= 1, x_1(2) = 1, x_1(3) = 1, x_1(4) = 1 \\ x_2(1) &= 1, x_2(2) = i, x_2(3) = -i, x_2(4) = -1 \\ x_3(1) &= 1, x_3(2) = -i, x_3(3) = i, x_3(4) = -1 \\ x_4(1) &= 1, x_4(2) = -1, x_4(3) = -1, x_4(4) = 1. \end{aligned}$$

Θεώρημα 1.2.6. (Σχέσεις ορθογωνιότητας χαρακτήρων Dirichlet) Έστω $q \in \mathbb{N}$. Τότε, ισχύουν τα ακόλουθα:

(i) Για κάθε χαρακτήρα Dirichlet modulo q ισχύει ότι

$$\sum_{m=1}^q x(m) = \begin{cases} \phi(q) & , \text{ αν } x = x_0 \\ 0 & , \text{ αν } x \neq x_0, \end{cases}$$

όπου x_0 είναι ο πρωταρχικός χαρακτήρας Dirichlet modulo q .

(ii) Για κάθε $m \in \mathbb{N}$ έχουμε ότι

$$\sum_{x \pmod{q}} x(m) = \begin{cases} \phi(q) & , \text{ αν } m \equiv 1 \pmod{q} \\ 0 & , \text{ αν } m \not\equiv 1 \pmod{q}, \end{cases}$$

όπου το άθροισμα είναι πάνω από όλους τους χαρακτήρες Dirichlet modulo q .

(iii) Για κάθε ζεύγος x_1, x_2 χαρακτήρων *Dirichlet modulo* q ισχύει

$$\sum_{m=1}^q x_1(m) \overline{x_2(m)} = \begin{cases} \phi(q) & , \text{αν } x_1 = x_2 \\ 0 & , \text{αν } x_1 \neq x_2. \end{cases}$$

(iv) Για κάθε $m, n \in \mathbb{N}$ έχουμε

$$\sum_{x \bmod q} x(m) \overline{x(n)} = \begin{cases} \phi(q) & , \text{αν } n \equiv m \pmod{q} \text{ και } (n, q) = 1 \\ 0 & , \text{διαφορετικά,} \end{cases}$$

όπου το άθροισμα είναι πάνω από όλους τους χαρακτήρες *Dirichlet modulo* q .

Απόδειξη. (i) Συμβολίζουμε με $S = \sum_{m=1}^q x(m)$. Αν $x = x_0$, τότε προκύπτει άμεσα ότι $S = \phi(q)$.

Έστω $x \neq x_0$, τότε υπάρχει αριθμός a_1 τέτοιος ώστε $(a_1, q) = 1$ και $x(a_1) \neq 1$. Τώρα, παρατηρούμε ότι:

$$x(a_1)S = \sum_{1 \leq a < q; (a, q)=1} x(a_1)x(a) = \sum_{1 \leq a < q; (a, q)=1} x(a_1a) = \sum_{1 \leq b < q; (b, q)=1} x(b) = S.$$

Αφού, έχουμε υποθέσει ότι $x(a_1) \neq 1$, προκύπτει ότι $S = 0$.

(ii) Συμβολίζουμε με $S = \sum_{x \bmod q} x(m)$. Αν $(a, q) > 1$, τότε όλοι οι όροι είναι ίσοι με μηδέν και

έχουμε ότι $S = 0$. Αν $(a, q) = 1$ και $a \not\equiv 1 \pmod{q}$ τότε $x(a) = x(1) = 1$ για όλους τους χαρακτήρες modulo q και από την Πρόταση 1.2.4 έχουμε ότι $S = \phi(q)$.

Έστω τώρα ότι $(a, q) = 1$ με $a \not\equiv 1 \pmod{q}$. Από την Πρόταση 1.2.4 υπάρχει χαρακτήρας x_1 περιόδου q τέτοιος ώστε $x_1(a) \neq 1$. Επειδή οι χαρακτήρες modulo q σχηματίζουν ομάδα, αν ο x διατρέχει όλους τους χαρακτήρες modulo q , το ίδιο κάνει και ο x_1x . Άρα, έχουμε:

$$x_1(a)S = \sum_{x \bmod q} x_1(a)x(a) = \sum_{x \bmod q} (x_1x)(a) = \sum_{\psi \bmod q} \psi(a) = S$$

και επειδή $x_1(a) \neq 1$, έπεται ότι $S = 0$.

(iii) Προκύπτει άμεσα από το (i) για τον χαρακτήρα $x = x_1 \overline{x_2}$ και με την παρατήρηση ότι $x = x_0$ αν και μόνο αν $x_1 = x_2$.

(iv) Υποθέτουμε ότι $(a_1, q) = (a_2, q) = 1$, διαφορετικά το άθροισμα είναι ίσο με μηδέν και έχουμε το ζητούμενο. Άρα, ο a_2 έχει πολλαπλασιαστικό αντίστροφο τον $\overline{a_2}$ modulo q . Έπειτα, εφαρμόζουμε το (ii) για $a = a_1 \overline{a_2}$. Παρατηρούμε ότι

$$x(a_2)x(a) = x(a_2a) = x(a_2a_1 \overline{a_2}) = x(a_1)$$

και έτσι

$$x(a) = \frac{x(a_1)}{x(a_2)} = x(a_1) \overline{x(a_2)}.$$

Τέλος, παρατηρούμε ότι $a = a_1 \overline{a_2} \equiv 1 \pmod{q}$ αν και μόνο αν $a_1 \equiv a_2 \pmod{q}$, και έχουμε το ζητούμενο. $\square$

Πόρισμα 1.2.7. Έστω $q \in \mathbb{N}$ και έστω x χαρακτήρας *Dirichlet modulo* q .

(i) Αν ο χαρακτήρας x δεν είναι ο πρωταρχικός χαρακτήρας x_0 modulo q , τότε

$$\left| \sum_{n \leq l} x(n) \right| \leq \phi(q)$$

για κάθε $l \geq 1$.

(ii) Αν $x = x_0$, τότε

$$\left| \sum_{n \leq l} x(n) - \frac{\phi(q)}{q} l \right| \leq 2\phi(q)$$

για κάθε $l \geq 1$.

Απόδειξη. Εφόσον ο χαρακτήρας *Dirichlet* x είναι q -περιοδική συνάρτηση, τότε για κάθε $l \geq 1$ ισχύει ότι

$$\sum_{n \leq l} x(n) = [l/q]S + R,$$

όπου

$$S = \sum_{a=1}^q x(a), |R| \leq \sum_{a=1}^q |x(a)|.$$

Προφανώς, $|R| \leq \phi(q)$ και από το (i) του Θεωρήματος 1.2.6 έχουμε ότι $S = 0$ αν $x \neq x_0$ και $S = \phi(q)$ αν $x = x_0$. Τέλος, τα δύο φράγματα προκύπτουν άμεσα από αυτές τις παρατηρήσεις. $\square$

Παρατηρήσεις 1.2.8. Με βάση το Πόρισμα 1.2.7, για την συνάρτηση $M(x, l) = \sum_{m \leq l} x(m)$, όπου $l \geq 1$ ισχύει ότι

$$M(x, l) = \begin{cases} O_q(1) & , \text{αν } x \neq x_0 \\ \frac{\phi(q)}{q} l + O_q(1) & , \text{αν } x = x_0. \end{cases}$$

Ορισμός 1.2.9. (*primitive* χαρακτήρας *Dirichlet*) Έστω x όχι πρωταρχικός χαρακτήρας *Dirichlet modulo* q . Αν για κάθε $n \in \mathbb{N}$, με $\mu(n, q) = 1$, ο αριθμός q είναι ο μικρότερος φυσικός k για τον οποίο ισχύει ότι $x(n+k) = x(n)$, λέμε ότι ο q είναι *conductor* του χαρακτήρα x , ενώ ο χαρακτήρας x ονομάζεται *primitive* χαρακτήρας *Dirichlet modulo* q . Διαφορετικά, υπάρχει μοναδικός φυσικός q_1 τέτοιος ώστε: $q_1 | q$ με $q_1 < q$ και υπάρχει x_1 *primitive* χαρακτήρας τέτοιος ώστε

$$x(n) = \begin{cases} x_1(n) & , \text{αν } (n, q) = 1 \\ 0 & , \text{αν } (n, q) > 1. \end{cases}$$

Σε αυτή την περίπτωση λέμε ότι:

- (i) Ο χαρακτήρας x είναι *impritive* χαρακτήρας του x_1
- (ii) Ο x_1 induces τον x .

1.3 Συνάρτηση L-Dirichlet

Ορισμός 1.3.1. (*Dirichlet L-συνάρτηση*) Έστω ένας χαρακτήρας Dirichlet x , και έστω μιγαδικός αριθμός $s = \sigma + it$, με τους σ και t να είναι πραγματικοί αριθμοί. Η συνάρτηση

$$L(s, x) = \sum_{n=1}^{\infty} \frac{x(n)}{n^s},$$

ονομάζεται *Dirichlet L-συνάρτηση* ή *Dirichlet L-σειρά* για τον χαρακτήρα x .

Θεώρημα 1.3.2. (*αναλυτικές ιδιότητες των L-συναρτήσεων*) Έστω x χαρακτήρας Dirichlet modulo q και έστω μιγαδικός αριθμός $s = \sigma + it$, με τους σ και t να είναι πραγματικοί αριθμοί. Συμβολίζουμε με $L(s, x)$ την *Dirichlet L-συνάρτηση* του χαρακτήρα x .

- (i) Αν $x \neq x_0$, όπου x_0 ο πρωταρχικός χαρακτήρας modulo q , τότε η $L(s, x)$ έχει αναλυτική συνέχιση στο ημιεπίπεδο $\sigma > 0$.
- (ii) Αν $x = x_0$, τότε $L(s, x)$ έχει απλό πόλο στο $s = 1$ με υπόλοιπο $\phi(q)/q$ και έχει αναλυτική συνέχιση σε όλα τα άλλα σημεία του ημιεπιπέδου $\sigma > 0$.

Απόδειξη. (i) Αν $x \neq x_0$ χρησιμοποιώντας μερική άθροιση και το γεγονός ότι τα μερικά αθροίσματα $\sum_{n \leq x} x(n)$ είναι πεπερασμένα, βλέπουμε εύκολα ότι η $L(s, x)$ συγκλίνει στο ημιεπίπεδο $\sigma > 0$. Επειδή, η σειρά Dirichlet είναι αναλυτική στο ημιεπίπεδο που συγκλίνει έχουμε και το ζητούμενο.

- (ii) Αν $x = x_0$ χρησιμοποιώντας παρόμοια επιχειρήματα για την αριθμητική συνάρτηση $f(n) = x_0(n) - \phi(q)/q$. Από την Παρατήρηση 1.2.8 τα μερικά αθροίσματα $\sum_{n \leq x} f(n)$ είναι φραγμένα και έτσι η σειρά Dirichlet $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ συγκλίνει στο ημιεπίπεδο $\sigma > 0$ και άρα αναλυτική σε αυτό. Από την άλλη έχουμε $x_0 = f(n) + \phi(q)$, άρα $L(s, x_0) = F(s) + (\phi(q)/q)\zeta(s)$ για $\sigma > 1$. Εφόσον, η $F(s)$ είναι αναλυτική στο $\sigma > 0$ και η $\zeta(s)$ είναι αναλυτική στο $\sigma > 0$ με εξαίρεση τον πόλο στο $s = 1$ με υπόλοιπο 1, συμπεραίνουμε ότι η $L(s, x_0)$ είναι αναλυτική στο $\sigma > 0$ με εξαίρεση τον πόλο στο $s = 1$ με υπόλοιπο $\phi(q)/q$.

□

1.4 Περιοδικές αριθμητικές συναρτήσεις και αθροίσματα Gauss

Ορισμός 1.4.1. (*Αριθμητική συνάρτηση*) Μια συνάρτηση f με πεδίο ορισμού τους φυσικούς και πεδίο τιμών ένα υποσύνολο ή όλο το μιγαδικό επίπεδο ονομάζεται *αριθμητική συνάρτηση*.

Ορισμός 1.4.2. (*Περιοδική αριθμητική συνάρτηση*) Έστω q θετικός ακέραιος. Μια αριθμητική συνάρτηση f λέγεται *περιοδική* με περίοδο q (ή *περιοδική modulo q*), αν

$$f(n + q) = f(n)$$

για κάθε $n \in \mathbb{N}$. Αν q είναι περίοδος το ίδιο είναι και ο mq για κάθε $m \in \mathbb{N}$. Η ελάχιστη περίοδος της f ονομάζεται *θεμελιώδης περίοδος*.

Οι χαρακτήρες Dirichlet περιόδου q είναι παραδείγματα αριθμητικών περιοδικών συναρτήσεων, διότι εξ' ορισμού τους ισχύει ότι

$$x(n+q) = x(n)$$

για κάθε $n \in \mathbb{N}$.

Άλλο ένα παράδειγμα είναι η εκθετική συνάρτηση

$$f(n) = e^{2\pi i m n / q},$$

όπου m, q σταθεροί ακέραιοι. Ο αριθμός $e^{2\pi i m / q}$ είναι μια q -οστή ρίζα της μονάδας και η $f(n)$ είναι η n -οστή δύναμη της. Κάθε πεπερασμένος συνδιασμός τέτοιων συναρτήσεων

$$\sum_m c(m) e^{2\pi i m n / q}$$

είναι επίσης περιοδικός modulo q , για κάθε επιλογή συντελεστών $c(m)$. Μάλιστα, μπορεί να αποδειχθεί ότι κάθε αριθμητική συνάρτηση περιόδου q , μπορεί να εκφραστεί ως γραμμικός συνδυασμός αυτού. Τα αθροίσματα αυτά ονομάζονται πεπερασμένες σειρές Fourier.

Πράγματι, αρχίζουμε την μελέτη με ένα απλό αλλά σημαντικό παράδειγμα, γνωστό ως γεωμετρικό άθροισμα.

Θεώρημα 1.4.3. Για ακέραιο $q \geq 1$, ορίζουμε την συνάρτηση $g : \mathbb{N} \rightarrow \mathbb{C}$ με τύπο

$$g(n) = \sum_{m=0}^{q-1} e^{2\pi i m n / q}.$$

Τότε

$$g(n) = \begin{cases} 0 & , \text{αν } q \nmid n \\ q & , \text{αν } q | n. \end{cases}$$

Απόδειξη. Επειδή $g(n)$ είναι το άθροισμα των όρων μιας γεωμετρικής προόδου, δηλαδή

$$g(n) = \sum_{m=0}^{q-1} x^m,$$

όπου $x = e^{2\pi i n / q}$, έπεται ότι

$$g(n) = \begin{cases} \frac{x^q - 1}{x - 1} & , \text{αν } x \neq 1 \\ q & , \text{αν } x = 1. \end{cases}$$

Αλλά: $x^q = 1$, και $x = 1$ αν και μόνο αν $q | n$, οπότε το θεώρημα απεδείχθη. □

Στην συνέχεια θα χρησιμοποιήσουμε τον πολυωνυμικό τύπο παρεμβολής του Langrange για να αποδείξουμε ότι κάθε περιοδική αριθμητική συνάρτηση έχει πεπερασμένο ανάπτυγμα Fourier.

Θεώρημα 1.4.4. (Θεώρημα παρεμβολής του Langrange) Έστω ότι $z_0, z_1, \dots, z_{q-1}$ είναι q διαφορετικοί μιγαδικοί αριθμοί, ενώ $w_0, w_1, \dots, w_{q-1}$ είναι q μιγαδικοί αριθμοί, που δεν είναι κατ' ανάγκη διαφορετικοί. Τότε υπάρχει ένα μοναδικό πολυώνυμο $P(z)$ βαθμού το πολύ $q - 1$, τέτοιο ώστε

$$P(z_m) = w_m$$

για $m = 0, 1, \dots, q - 1$.

Απόδειξη. Το ζητούμενο πολυώνυμο $P(z)$ ονομάζεται πολυώνυμο παρεμβολής του Langrange και μπορεί να κατασκευαστεί ως εξής: Έστω

$$A(z) = (z - z_0)(z - z_1) \cdot \dots \cdot (z - z_{q-1})$$

και έστω

$$A_m(z) = \frac{A(z)}{z - z_m}.$$

Τότε το $A_m(z)$ είναι πολυώνυμο βαθμού $q - 1$ με τις ακόλουθες ιδιότητες:

- $A_m(z_m) \neq 0$,
- $A_m(z_j) = 0$ αν $j \neq m$.

Επομένως, το $A_m(z)/A_m(z_m)$ είναι πολυώνυμο βαθμού $q - 1$, που μηδενίζει σε κάθε z_j για $j \neq m$ και έχει την τιμή 1 στο z_m . Επομένως, ο γραμμικός συνδιασμός

$$P(z) = \sum_{m=0}^{q-1} w_m \frac{A_m(z)}{A_m(z_m)}$$

είναι πολυώνυμο βαθμού $\leq q - 1$ με $P(z_j) = w_j$ για κάθε j . Αν υπήρχε άλλο τέτοιο πολυώνυμο, έστω $Q(z)$, τότε η διαφορά $P(z) - Q(z)$ θα μηδενιζόταν σε q διαφορετικά σημεία, οπότε $P(z) = Q(z)$ γιατί τα δύο πολυώνυμα έχουν βαθμό $\leq q - 1$. $\square$

Επιλέγουμε τώρα τους αριθμούς $z_0, z_1, \dots, z_{q-1}$ ώστε να είναι οι q -οστές ρίζες της μονάδας οπότε προκύπτει το ακόλουθο:

Θεώρημα 1.4.5. Για δοσμένους q μιγαδικούς αριθμούς $w_0, w_1, \dots, w_{q-1}$, υπάρχουν q μονοσήμαντα ορισμένοι μιγαδικοί αριθμοί $a_0, a_1, \dots, a_{q-1}$ τέτοιοι ώστε

$$w_m = \sum_{n=0}^{q-1} a_n e^{2\pi i m n / q} \quad (1.8)$$

για $m = 0, 1, \dots, q - 1$. Ακόμη, οι συντελεστές a_n δίνονται από τον τύπο:

$$a_n = \frac{1}{q} \sum_{m=0}^{q-1} w_m e^{-2\pi i m n / q} \quad (1.9)$$

για $n = 0, 1, \dots, q - 1$.

Απόδειξη. Έστω $z_m = e^{2\pi im/q}$. Οι αριθμοί $z_0, \dots, z_{q-1}$ είναι διαφορετικοί, οπότε υπάρχει μοναδικό πολυώνυμο Lagrange

$$P(z) = \sum_{n=0}^{q-1} a_n z^n$$

τέτοιο ώστε $P(z_m) = w_m$ για κάθε $m = 0, \dots, q-1$. Αυτό αποδεικνύει ότι υπάρχουν μοναδικοί αριθμοί a_n , που ικανοποιούν την (1.8). Για να συνεπάγουμε την (1.9) για τους a_n , πολλαπλασιάζουμε τα μέλη της (1.8) με $e^{-2\pi imr/q}$, όπου m και r είναι μη αρνητικοί ακέραιοι, μικρότεροι από τον q και αθροίζουμε ως προς τον δείκτη m , οπότε προκύπτει:

$$\sum_{m=0}^{q-1} w_m e^{-2\pi imr/q} = \sum_{n=0}^{q-1} a_n \sum_{m=0}^{q-1} e^{2\pi i(n-r)m/q}.$$

Κατά το Θεώρημα 1.4.3, το άθροισμα ως προς m είναι μηδέν, εκτός εάν $q|(n-r)$. Αλλά $|n-r| \leq q-1$, οπότε $q|(n-r)$ τότε και μόνο τότε αν $n=r$. Επομένως, ο μόνος μη μηδενικός όρος στα δεξιά εμφανίζεται για $n=r$, οπότε βρίσκουμε:

$$\sum_{m=0}^{q-1} w_m e^{-2\pi imr/q} = qa_r.$$

Η εξίσωση αυτή μας δίνει την (1.9). □

Θεώρημα 1.4.6. Έστω f μία αριθμητική συνάρτηση q -περιοδική. Τότε, υπάρχει μοναδική αριθμητική συνάρτηση g , που είναι q -περιοδική και ικανοποιεί

$$f(m) = \sum_{n=0}^{q-1} g(n) e^{2\pi imn/q}.$$

Η συνάρτηση g δίνεται από τον τύπο

$$g(n) = \sum_{m=0}^{q-1} f(m) e^{-2\pi imn/q}.$$

Απόδειξη. Έστω $w_m = f(m)$ για $m = 0, 1, \dots, q-1$. Εφαρμόζουμε το Θεώρημα 1.4.5 για να προσδιορίσουμε τους αριθμούς $a_0, \dots, a_{q-1}$. Ας ορίσουμε την συνάρτηση g με τις σχέσεις $g(m) = a_m$ για $m = 0, 1, \dots, q-1$ και ας επεκτείνουμε τον ορισμό της $g(m)$ για όλους τους ακέραιους m μέσω της περιοδικότητας $\text{mod } q$. Τότε, η f σχετίζεται με την g μέσω των εξισώσεων του θεωρήματος. □

Σημείωση: Επειδή οι συναρτήσεις f, g είναι q -περιοδικές, τα αθροίσματα του θεωρήματος 1.4.6 μπορούν να ξαναγραφτούν ως:

$$f(m) = \sum_{n \text{ mod } q} g(n) e^{2\pi imn/q}$$

και

$$g(n) = \sum_{m \text{ mod } q} f(m) e^{-2\pi imn/q}.$$

Σε κάθε περίπτωση το άθροισμα μπορεί να επεκταθεί σε οποιοδήποτε πλήρες σύστημα υπολοίπων modulo q . Το άθροισμα με το οποίο ισούτε η f ονομάζεται ανάπτυγμα κατά Fourier της f , ενώ οι αριθμοί $g(n)$ ονομάζονται συντελεστές Fourier της f .

Ορισμός 1.4.7. (Άθροισμα Gauss) Για κάθε χαρακτήρα Dirichlet x modulo q , το άθροισμα

$$G(n, x) = \sum_{m=1}^q x(m) e^{2\pi i m n / q}$$

ονομάζεται άθροισμα Gauss, αντίστοιχο στον x .

Θεώρημα 1.4.8. Αν x ένας οποιοδήποτε χαρακτήρας Dirichlet modulo q , τότε

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

,όταν $(n, q) = 1$.

Απόδειξη. Όταν $(n, q) = 1$, οι αριθμοί nr διατρέχουν ένα πλήρες σύστημα mod q για τις διάφορες τιμές του r . Επίσης, $|x(n)|^2 = x(n)\overline{x(n)} = 1$, οπότε

$$x(r) = \overline{x(n)} x(n) x(r) = \overline{x(n)} x(nr).$$

Επομένως, το άθροισμα που ορίζει το $G(n, x)$, μπορεί να γραφεί ως εξής:

$$\begin{aligned} G(n, x) &= \sum_{r \bmod q} x(r) e^{2\pi i nr / q} = \overline{x(n)} \sum_{r \bmod q} x(nr) e^{2\pi i nr / q} \\ &= \overline{x(n)} \sum_{m \bmod q} x(m) e^{2\pi i m / q} = \overline{x(n)} G(1, x). \end{aligned}$$

Αυτό αποδεικνύει το θεώρημα. □

Ορισμός 1.4.9. (Διαχωρίσιμο άθροισμα Gauss) Το άθροισμα Gauss $G(n, x)$ λέγεται διαχωρίσιμο, αν ισχύει

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

Θεώρημα 1.4.10. Αν το $G(x, n)$ είναι διαχωρίσιμο για κάθε n , τότε ισχύει:

$$|G(1, x)|^2 = q$$

όπου q η περίοδος του χαρακτήρα x .

Απόδειξη. Έχουμε:

$$|G(1, x)|^2 = G(1, x) \overline{G(1, x)} = G(1, x) \sum_{m=1}^q \overline{x(m)} e^{-2\pi i m / q}$$

$$\begin{aligned}\sum_{m=1}^q G(m, x) e^{-2\pi i m/q} &= \sum_{m=1}^q \sum_{r=1}^q x(r) e^{2\pi i m r/q} e^{-2\pi i m/q} \\ &= \sum_{r=1}^q x(r) \sum_{m=1}^q e^{2\pi i m(r-1)/q} = qx(1) = q,\end{aligned}$$

γιατί το τελευταίο άθροισμα ως προς m είναι γεωμετρικό άθροισμα, που μηδενίζεται, εκτός αν $r = 1$. $\square$

Από το ότι κάθε χαρακτήρας Dirichlet x modulo q είναι q περιοδική αριθμητική συνάρτηση, έχει πεπερασμένο ανάπτυγμα κατά Fourier

$$x(m) = \sum_{n=1}^q a_q(n) e^{2\pi i m n/q},$$

ενώ το θεώρημα 1.4.6 μας λέει ότι οι συντελεστές δίνονται από τον τύπο

$$a_q(n) = \frac{1}{q} \sum_{m=1}^q x(m) e^{-2\pi i m n/q}.$$

Το άθροισμα στα δεξιά είναι το άθροισμα Gauss $G(-n, x)$, οπότε έχουμε

$$a_q(n) = \frac{1}{q} G(-n, x).$$

Μάλιστα, όταν ο χαρακτήρας είναι primitive, το ανάπτυγμα Fourier μπορεί να εκφραστεί ως εξής:

Θεώρημα 1.4.11. Το πεπερασμένο ανάπτυγμα Fourier ενός primitive χαρακτήρα Dirichlet x modulo q έχει την μορφή

$$x(m) = \frac{\tau_q(x)}{\sqrt{q}} \sum_{n=1}^q \bar{x}(n) e^{-2\pi i m n/q},$$

όπου

$$\tau_q(x) = \frac{G(1, x)}{\sqrt{q}} = \frac{1}{\sqrt{q}} \sum_{m=1}^q x(m) e^{2\pi i m/q}.$$

Οι αριθμοί $\tau_q(x)$ έχουν απόλυτη τιμή ίση με 1.

Απόδειξη. Επειδή, ο x είναι primitive χαρακτήρας Dirichlet έχουμε ότι $G(-n, x) = \bar{x}(-n)G(1, x)$ και έτσι οι συντελεστές μπορούν να γραφούν ως $a_q(n) = \bar{x}(-n)G(1, x)/q$. Επομένως, για την σειρά Fourier έχουμε:

$$x(m) = \frac{G(1, x)}{q} \sum_{n=1}^q \bar{x}(-n) e^{2\pi i m n/q} = \frac{G(1, x)}{q} \sum_{n=1}^q \bar{x}(n) e^{-2\pi i m n/q},$$

που είναι και το ζητούμενο. Από το θεώρημα 1.4.10 έπεται ότι οι αριθμοί $\tau_q(x)$ έχουν απόλυτη τιμή ίση με 1. $\square$

1.5 Σειρές Dirichlet και γινόμενα Euler

Ορισμός 1.5.1. (Πολλαπλασιαστική συνάρτηση) Μια αριθμητική συνάρτηση $f : \mathbb{N} \rightarrow \mathbb{C}$ ονομάζεται πολλαπλασιαστική αν δεν είναι ταυτοτικά μηδέν και εάν ισχύει

$$f(mn) = f(m)f(n),$$

οποτεδήποτε $(m, n) = 1$.

Ορισμός 1.5.2. (Πλήρως πολλαπλασιαστική συνάρτηση) Μια πολλαπλασιαστική συνάρτηση $f : \mathbb{N} \rightarrow \mathbb{C}$ ονομάζεται πλήρως πολλαπλασιαστική εάν επιπλέον ισχύει

$$f(mn) = f(m)f(n)$$

για κάθε $m, n \in \mathbb{N}$.

Ορισμός 1.5.3. (Σειρά Dirichlet) Έστω μια αριθμητική συνάρτηση $f : \mathbb{N} \rightarrow \mathbb{C}$ και έστω μιγαδικός αριθμός $s = \sigma + it$, με τους σ και t να είναι πραγματικοί αριθμοί. Μια σειρά της μορφής

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

λέγεται σειρά Dirichlet με συντελεστές $f(n)$.

Θεώρημα 1.5.4. (Γινόμενο Euler) Έστω μια πολλαπλασιαστική συνάρτηση, τέτοια ώστε η σειρά $\sum_n f(n)$ να συγκλίνει απόλυτα. Τότε, το άθροισμα της σειράς μπορεί να εκφραστεί ως απειρογινόμενο που συγκλίνει απόλυτα, δηλαδή

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + \dots) \quad (1.10)$$

εκτιμώμενο πάνω σε όλους τους πρώτους p . Αν επιπλέον η συνάρτηση f είναι πλήρως πολλαπλασιαστική, τότε το απειρογινόμενο απλουστεύεται και ισχύει

$$\sum_{n=1}^{\infty} f(n) = \prod_p \frac{1}{1 - f(p)}. \quad (1.11)$$

Απόδειξη. Ας θεωρήσουμε το πεπερασμένο γινόμενο

$$P(x) = \prod_{p \leq x} \{1 + f(p) + f(p^2) + \dots\}$$

πάνω από όλους τους πρώτους $p \leq x$. Επειδή αυτό είναι το γινόμενο ενός πεπερασμένου πλήθους σειρών, που συγκλίνουν απόλυτα, έπεται από ότι μπορούμε να πολλαπλασιάσουμε αυτές τις σειρές και να αναδιατάξουμε τους όρους, κατά οποιοδήποτε τρόπο, χωρίς να μεταβληθεί το άθροισμα.

Επειδή η f είναι πολλαπλασιαστική, ένας τυπικός όρος είναι της μορφής

$$f(p_1^{a_1}) \cdot \dots \cdot f(p_r^{a_r}) = f(p_1^{a_1} \cdot \dots \cdot p_r^{a_r}).$$

Κατά το θεμελιώδες θεώρημα της Αριθμητικής, μπορούμε να γράψουμε

$$P(x) = \sum_{n \in A} f(n),$$

όπου το σύνολο A αποτελείται από τους φυσικούς αριθμούς n , των οποίων όλοι οι πρώτοι παράγοντες είναι $\leq x$. Κατά συνέπεια:

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B} f(n),$$

όπου B είναι το σύνολο των φυσικών αριθμών n , με έναν τουλάχιστον πρώτο παράγοντα $> x$. Επομένως,

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \leq \sum_{n \in B} |f(n)| \leq \sum_{n > x} |f(n)|.$$

Τώρα, για $x \rightarrow \infty$ το τελευταίο άθροισμα στα δεξιά τείνει στο 0, διότι η σειρά $\sum |f(n)|$ συγκλίνει. Κατά συνέπεια

$$P(x) \rightarrow \sum f(n)$$

για $x \rightarrow \infty$.

Τώρα ένα απειρογινόμενο της μορφής $\prod (1 + a_n)$ συγκλίνει απόλυτα, όταν η αντίστοιχη σειρά $\sum a_n$ συγκλίνει απόλυτα. Στην περίπτωση αυτή έχουμε

$$\sum_{p \leq x} |f(p)| + |f(p^2)| + \dots \leq \sum_{p \leq x} (|f(p)| + |f(p^2)| + \dots) \leq \sum_{n=2} |f(n)|.$$

Επειδή τα μερικά αθροίσματα είναι φραγμένα, έπεται ότι η σειρά των θετικών όρων

$$\sum_p |f(p) + f(p^2) + \dots|$$

συγκλίνει και αυτό συνεπάγεται την απόλυτη σύγκλιση του γινομένου στην (1.10).

Τέλος, όταν η f είναι πλήρως πολλαπλασιαστική έχουμε $(f(p^n) = f(p)^n$, ενώ κάθε σειρά στο μέλος της (1.10) είναι μια συγκλίνουσα γεωμετρική σειρά με άθροισμα $(1 - f(p))^{-1}$. $\square$

Θεώρημα 1.5.5. Έστω ότι η σειρά *Dirichlet* $\sum_n \frac{f(n)}{n^s}$, με $s = \sigma + it$, συγκλίνει απόλυτα για $\sigma > \sigma_a$. Αν η σειρά f είναι πολλαπλασιαστική, τότε ισχύει:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots \right)$$

για $\sigma > \sigma_a$. Αν επιπλέον η συνάρτηση f είναι πλήρως πολλαπλασιαστική, τότε ισχύει ότι:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - f(p)p^{-s}},$$

για $\sigma > \sigma_a$.

Απόδειξη. Εφαρμόζοντας τώρα το θεώρημα 1.5.4 σε απόλυτα συγκλίνουσες σειρές *Dirichlet*, συνάγουμε αμέσως το ζητούμενο. $\square$

Παραδείγματα 1.5.6. Έστω μιγαδικός αριθμός $s = \sigma + it$, με τους σ και t να είναι πραγματικοί αριθμοί.

(i) **Riemann zeta function**

Το πιο γνωστό παράδειγμα γινομένου *Euler* είναι αυτό της συνάρτησης ζήτα του *Riemann*, δηλαδή της σειράς *Dirichlet* για την αριθμητική συνάρτηση $f(n) = 1$, $\forall n \in \mathbb{N}$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{1}{p^{ms}} \right) = \prod_p \left(1 - \frac{1}{p^s} \right)^{-1}, (\sigma > 1).$$

(ii) **Μη-πρωταρχικός χαρακτήρας Dirichlet**

Έστω ένας μη-πρωταρχικός χαρακτήρας *Dirichlet* x modulo q , τότε έχουμε

$$L(s, x) = \sum_{n=1}^{\infty} \frac{x(n)}{n^s} = \prod_p \left(1 - \frac{x(p)}{p^s} \right)^{-1}, (\sigma > 1).$$

(iii) **Πρωταρχικός χαρακτήρας Dirichlet**

Έστω ένας πρωταρχικός χαρακτήρας x_1 *Dirichlet* modulo q , τότε εξ' ορισμού έχουμε ότι $x_1(p) = 0$ για κάθε $p|q$ και $x_1(p) = 1$ για κάθε $p \nmid q$. Τότε το γινόμενο *Euler* γίνεται:

$$L(s, x_1) = \prod_{p \nmid q} \frac{1}{1 - p^{-s}} = \prod_p \frac{1}{1 - p^{-s}} \cdot \prod_{p|q} (1 - p^{-s}) = \zeta(s) \prod_{p|q} (1 - p^{-s}).$$

Έτσι η L - συνάρτηση $L(s, x_1)$ ισούται με την συνάρτηση ζήτα $\zeta(s)$ πολλαπλασιασμένη επί ένα πεπερασμένο πλήθος παραγόντων.

1.6 Εκτιμήσεις Merten's

Ορισμός 1.6.1. (Συνάρτηση (von) Mangoldt $\Lambda(n)$) Για κάθε ακέραιο $n \geq 1$ ορίζουμε

$$\Lambda(n) = \log p,$$

όταν $n = p^m$ για κάποιο πρώτο p και για κάποιο ακέραιο $m \geq 1$. Ενώ,

$$\lambda(n) = 0$$

σε κάθε άλλη περίπτωση.

Θεώρημα 1.6.2. Για κάθε ακέραιο $n \geq 1$ ισχύει ότι

$$\log n = \sum_{d|n} \Lambda(d). \quad (1.12)$$

Απόδειξη. Το θεώρημα αληθεύει για $n = 1$, επειδή και τα δύο μέλη της (1.12) είναι 0. Για $n > 1$, τον αναλύουμε σε γινόμενο πρώτων παραγόντων:

$$n = p_1^{a_1} \cdot \dots \cdot p_r^{a_r}.$$

Παίρνοντας λογαρίθμους έχουμε

$$\log n = a_1 \log p_1 + \dots + a_r \log p_r.$$

Τώρα, ας θεωρήσουμε το άθροισμα στο δεξιό μέλος της (1.12). Στο άθροισμα αυτό οι μόνοι μη μηδενικοί όροι προέρχονται από τους διαιρέτες d της μορφής p_k^m για $m = 1, 2, \dots, a_k$ και $k = 1, 2, \dots, r$. Επομένως,

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^r \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^r \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^r a_k \log p_k = \log n,$$

που αποδεικνύει την (1.12). □

Στην συνέχεια, για να δώσουμε τις εκτιμήσεις του Merten's, απαραίτητο εργαλείο είναι οι εκτιμήσεις του Chebyshev, για τις οποίες θα χρειαστούμε τους εξής ορισμούς:

Ορισμός 1.6.3. Έστω $x \geq 1$. Τότε, ορίζουμε τις συναρτήσεις:

$$(i) \quad \pi(x) = \sum_{p \leq x} 1,$$

δηλαδή το πλήθος των πρώτων που δεν ξεπερνούν τον αριθμό x .

$$(ii) \quad \theta(x) = \sum_{p \leq x} \log p.$$

$$(iii) \quad \psi(x) = \sum_{n \leq x} \Lambda(n).$$

Στην συνέχεια έχουμε το θεώρημα για τις εκτιμήσεις Chebyshev, η απόδειξη δίνεται στο [4] σελίδα 83.

Θεώρημα 1.6.4. (Εκτιμήσεις Chebyshev) Για $x \geq 2$ έχουμε:

$$(i) \psi(x) \asymp x.$$

$$(ii) \theta(x) \asymp x.$$

$$(iii) \pi(x) \asymp \frac{x}{\log x}.$$

Τέλος, δίνουμε τις εκτιμήσεις του εκτιμήσεις Mertens's, η απόδειξη δίνεται στο [4] σελίδα 88.

Θεώρημα 1.6.5. (Εκτιμήσεις Mertens's) Για κάθε $x \geq 2$ ισχύουν τα παρακάτω:

$$(i) \sum_{n \leq x} \frac{\Lambda(x)}{n} = \log x + O(1),$$

$$(ii) \sum_{p \leq x} \frac{\log p}{p} = \log x + O(1),$$

$$(iii) \sum_{p \leq x} \frac{1}{p} = \log \log x + A + O\left(\frac{1}{\log x}\right),$$

$$(iv) \text{ (Θεώρημα Mertens's)}$$

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x} \left(1 + O\left(\frac{1}{\log x}\right)\right),$$

,όπου το A είναι μια σταθερά και γ είναι η σταθερά του Euler.

Σημείωση: Θα χρησιμοποιήσουμε και την εξής ισοδύναμη μορφή του (iv):

$$(iv') \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma(\log x)} \left(1 + O\left(\frac{1}{\log x}\right)\right).$$

2 Στοιχεία ανάλυσης

Σε αυτή την παράγραφο θα δόσουμε βασικούς ορισμούς και αποτελέσματα πάνω σε κάποια βασικά εργαλεία της ανάλυσης πάνω στα μέτρα τα οποία είναι ορισμένα σε χώρους πιθανότητας (μας ενδιαφέρει κυρίως το θεώρημα Prokhorov και η ασθενής σύγκριση μέτρων πιθανότητας), καθώς και μία βασική ταυτότητα πάνω στον διακριτό μετασχηματισμό κτιμήσεις Fourier.

2.1 Θεώρημα Prokhorov

Ορισμός 2.1.1. Έστω ένας χώρος S μετρικός χώρος και έστω $\mathcal{S}$ η Borel σ -άλγεβρα που παράγεται από τα ανοιχτά σύνολα του S και έστω ένα μέτρο P στην σ -άλγεβρα $\mathcal{S}$ τέτοιο ώστε

$$P(S) = 1.$$

Τότε, το μέτρο P ονομάζεται μέτρο πιθανότητας, ενώ η τριάδα

$$(S, \mathcal{S}, P)$$

ονομάζεται χώρος πιθανότητας.

Στην συνέχεια δίνουμε κάποιες βασικές ιδιότητες των μέτρων πιθανότητας.

Ορισμός 2.1.2. (κανονικό μέτρο πιθανότητας) Ένα μέτρο πιθανότητας P πάνω στον μετρήσιμο χώρο $(S, \mathcal{S})$ ονομάζεται κανονικό αν για κάθε $A \in \mathcal{S}$ και για κάθε $\varepsilon > 0$ υπάρχει κλειστό $F \in \mathcal{S}$ και υπάρχει ανοιχτό $G \in \mathcal{S}$ τέτοια ώστε $F \subset A \subset G$ και $P(G - F) < \varepsilon$.

Θεώρημα 2.1.3. Κάθε μέτρο πιθανότητας P στο $(S, \mathcal{S})$ είναι κανονικό.

Απόδειξη. Στον χώρο S ορίζουμε την μετρική $r(x, y)$ και την απόσταση του x από το A με $r(x, A)$. Αν το A είναι κλειστό μπορούμε να πάρουμε $F = A$ και $G = A^\delta = \{x : r(x, A) < \delta\}$ για κάποιο $\delta > 0$ και αυτά τα σύνολα φθίνουν προς το A , καθώς $\delta \downarrow 0$. Επομένως αρκεί να δείξουμε ότι η κλάση $\mathcal{G}$ που αποτελείται από τα S -σύνολα με την παραπάνω ιδιότητα, είναι σ -field.

Για δοθείσα ακολουθία συνόλων A_n στην κλάση $\mathcal{G}$ διαλέγουμε ακολουθία κλειστών συνόλων F_n και ακολουθία ανοιχτών συνόλων G_n τέτοια ώστε $F_n \subset A_n \subset G_n$ και $P(G_n - F_n) < \varepsilon/2^{n+1}$. Αν $G = \bigcup_n G_n$ και αν $F = \bigcup_{n \leq n_0} F_n$, με $n_0 \in \mathbb{N}$ τέτοιο ώστε $P(\bigcup_n F_n - F) < \varepsilon/2$, τότε έχουμε $F \subset \bigcup_n A_n \subset G$ και $P(G - F) < \varepsilon$. Επομένως η κλάση $\mathcal{G}$ είναι κλειστή κάτω από αριθμήσιμες ενώσεις, καθώς είναι κλειστή στα συμπληρώματα, δηλαδή $\mathcal{G}$ είναι σ -field. $\square$

Συμβολισμός Έστω P μέτρο πιθανότητας στον μετρήσιμο $(S, \mathcal{S})$ και έστω μια συνάρτηση $f : S \rightarrow \mathbb{R}$, τότε με τον συμβολισμό Pf εννοούμε

$$Pf = \int_S f(s) dP(s).$$

Θεώρημα 2.1.4. Δύο μέτρα πιθανότητας P και Q στην $\mathcal{S}$ συμπίπτουν αν $Pf = Qf$ για όλες τις φραγμένες, ομοιόμορφα συνεχείς πραγματικές συναρτήσεις f .

Απόδειξη. Έστω F κλειστό, θεωρούμε την συνάρτηση $f(x) = (1 - r(x, F)/\varepsilon)^+ = (1 - r(x, F)/\varepsilon) \cdot 1_A(x)$, όπου 1_A η χαρακτηριστική του συνόλου $A = \{x \in S, (1 - r(x, F)/\varepsilon) \geq 0\}$. Τότε, η f είναι φραγμένη, ομοιόμορφα συνεχής και για κάθε $x \in F$ ισχύει ότι $f(x) = 1$ ενώ για κάθε $x \notin F^\varepsilon$ έχουμε ότι $r(x, F) \geq \varepsilon$ και έτσι $f(x) = 0$. Ειδικότερα

$$I_F(x) \leq f(x) \leq I_{F^\varepsilon}(x).$$

Για αυτή την f έχουμε ότι

$$PF \leq Pf = Qf \leq QF^\varepsilon.$$

Αφήνοντας $\varepsilon \downarrow 0$ έχουμε $PF \leq QF$ για F κλειστό. Από συμμετρία και το θεώρημα 2.1.3 έπεται ότι $P = Q$. $\square$

Ο παρακάτω ορισμός, για τα tight μέτρα πιθανότητας, είναι πολύ χρήσιμος τόσο στην θεωρία της ασθενούς σύγκλισης των μέτρων όσο και στο θεώρημα Prokhorov.

Ορισμός 2.1.5. (tight μέτρο πιθανότητας) Ένα μέτρο πιθανότητας P στον μετρήσιμο χώρο $(S, \mathcal{S})$ ονομάζεται tight αν για κάθε $\varepsilon > 0$ υπάρχει συμπαγές σύνολο K τέτοιο ώστε $P(K) > 1 - \varepsilon$. Με βάση το Θεώρημα 2.1.3, ισοδύναμα έχουμε ότι:

P είναι tight αν και μόνο αν για κάθε $A \in \mathcal{S}$ ισχύει ότι

$$P(A) = \sup_{K \in B} P(K),$$

όπου για το σύνολο $B = \{K \subset A : K \text{ συμπαγές}\}$.

Θεώρημα 2.1.6. Αν ο μετρικός χώρος S είναι πλήρης και διαχωρίσιμος, τότε κάθε μέτρο πιθανότητας στον μετρήσιμο χώρο $(S, \mathcal{S})$ είναι tight.

Απόδειξη. Εφόσον το S είναι διαχωρίσιμο υπάρχει, για κάθε k , μια ακολουθία ανοιχτών $1/k$ -μπαλών $A_{k_1}, A_{k_2}, \dots$ που καλύπτουν το S . Για αρκετά μεγάλο n_k μπορούμε να πετύχουμε

$$P(\cup_{i \leq n_k} A_{k_i}) > 1 - \varepsilon/2^k.$$

Από την υπόθεση της πληρότητας, το σύνολο $\cap_{k \geq 1} \cup_{i \leq n_k} A_{k_i}$ έχει συμπαγές κλειστότητα το K , όμως προφανώς $PK > 1 - \varepsilon$. $\square$

Ορισμός 2.1.7. (ασθενής σύγκλιση μέτρων πιθανότητας) Έστω P και $(P_n)_{n \in \mathbb{N}}$ μέτρα πιθανότητας στον μετρήσιμο χώρο $(S, \mathcal{S})$. Λέμε ότι P_n συγκλίνει ασθενώς στο P και συμβολίζουμε $P_n \Rightarrow P$, αν για κάθε $f : S \rightarrow \mathbb{R}$ φραγμένη και συνεχής, ισχύει ότι

$$P_n f \rightarrow P f$$

καθώς $n \rightarrow \infty$.

Παρακάτω δίνεται ένας ισοδύναμος χαρακτηρισμός για την ασθενή σύγκλιση μέτρων πιθανότητας. Την απόδειξη μπορεί κάποιος να την βρει στο [2], σελίδα 16.

Θεώρημα 2.1.8. (Ισοδύναμος χαρακτηρισμός ασθενούς σύγκλισης) Έστω P και $(P_n)_{n \in \mathbb{N}}$ μέτρα πιθανότητας στον $(S, \mathcal{S})$. Τα ακόλουθα είναι ισοδύναμα:

- (i) $P_n \Rightarrow P$.
- (ii) $P_n f \rightarrow P f$, για κάθε φραγμένη και ομοιόμορφα συνεχής f .
- (iii) $\limsup_n P_n(F) \leq P(F)$, για κάθε F κλειστό.
- (iv) $\liminf_n P_n(G) \geq P(G)$, για κάθε G ανοιχτό.
- (v) $P_n(A) \rightarrow P(A)$, για κάθε P -συνεχές σύνολο A .

Ορισμός 2.1.9. (σχετική συμπαγεια μέτρων πιθανότητας) Έστω Π μια συλλογή μέτρων πιθανότητας στον $(S, \mathcal{S})$. Λέμε ότι το Π είναι σχετικά συμπαγές (relatively compact) αν για κάθε $(P_n)_{n \in \mathbb{N}}$ ακολουθία στοιχείων του Π υπάρχει υπακολουθία της (P_{n_j}) , που συγκλίνει ασθενώς σε ένα μέτρο Q στον $(S, \mathcal{S})$.

Στην συνέχεια δίνουμε το θεώρημα Prokhorov, η απόδειξη του οποίου βρίσκεται στο [2], σελίδα 60.

Θεώρημα 2.1.10. (Θεώρημα Prokhorov)

Έστω $(S, \mathcal{S})$, τότε ισχύει ότι:

- (i) Αν Π είναι μια συλλογή μέτρων πιθανότητας στον $(S, \mathcal{S})$ και είναι tight, τότε είναι σχετικά συμπαγής.
- (ii) Αν επιπλέον έχουμε ότι ο S είναι διαχωρίσιμος, τότε ισχύει και το αντίστροφο.

2.2 Ταυτότητα Plancherel

Ορισμός 2.2.1. (Διακριτός μετασχηματισμός Fourier)

Έστω μία ακολουθία N μιγαδικών αριθμών $\{x_n\} := (x_0, x_1, \dots, x_{N-1})$. Ο διακριτός μετασχηματισμός Fourier είναι μία συνάρτηση $\hat{F} : \mathbb{C}^N \rightarrow \mathbb{C}^N$ η οποία μετασχηματίζει την ακολουθία $\{x_n\}$ σε μία άλλη μιγαδική ακολουθία N όρων, την $\{X_k\} := (X_0, X_1, \dots, X_{N-1})$, με τύπο

$$X_k := \sum_{n=0}^{N-1} x_n e^{-2\pi i k n / N},$$

για κάθε $k \in \{0, 1, \dots, N-1\}$.

Ο ορισμός 2.2.1 μπορεί να χρησιμοποιηθεί και για ακολουθίες οι οποίες είναι N περιοδικές.

Ορισμός 2.2.2. (Αντίστροφος διακριτός μετασχηματισμός Fourier)

Ο αντίστροφος διακριτός μετασχηματισμός Fourier είναι μια γραμμική απεικόνιση $F : \mathbb{C}^N \rightarrow \mathbb{C}^N$ κατά την οποία, σύμφωνα με τον προηγούμενο συμβολισμό, δίνει

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{2\pi i k n / N}$$

για κάθε $n \in \{0, 1, \dots, N-1\}$.

Πρόταση 2.2.3. (Ταυτότητα Plancherel) Έστω $\{x_n\}$ και $\{X_k\}$ όπως πριν, τότε ισχύει ότι:

$$\sum_{n=0}^{N-1} |x_n|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |X_k|^2.$$

Απόδειξη. Σύμφωνα με τους παραπάνω ορισμούς έχουμε:

$$\begin{aligned} \frac{1}{N} \sum_{k=0}^{N-1} |X_k|^2 &= \frac{1}{N} \sum_{k=0}^{N-1} X_k \overline{X_k} = \frac{1}{N} \sum_{k=0}^{N-1} \left(\sum_{n=0}^{N-1} x(n) e^{-2\pi i k n / N} \right) \overline{X_k} = \\ &= \frac{1}{N} \sum_{n=0}^{N-1} \left(\sum_{k=0}^{N-1} \overline{X_k} e^{-2\pi i k n / N} \right) = \frac{1}{N} \sum_{n=0}^{N-1} x_n (N \cdot \overline{x_n}) = \\ &= \sum_{n=0}^{N-1} |x_n|^2. \end{aligned}$$

□

3 Εισαγωγή στο πρόβλημα discrepancy του Erdős

3.1 Κεντρικό θεώρημα

Ορισμός 3.1.1. (*Discrepancy συνάρτησης*) Έστω μία ακολουθία $f : \mathbb{N} \rightarrow \mathbb{H}$, όπου $\mathbb{H}$ μιγαδικός ή πραγματικός χώρος Hilbert. Ορίζουμε το *Discrepancy* της συνάρτησης f ως την ποσότητα

$$\sup_{n,d \in \mathbb{N}} \left\| \sum_{j=1}^n f(jd) \right\|_{\mathbb{H}}.$$

Ο κύριος στόχος είναι να αποδειχθεί το παρακάτω θεώρημα:

Θεώρημα 3.1.2. (*Το πρόβλημα discrepancy του Erdős για διανυσματικές τιμές*) Έστω $\mathbb{H}$ πραγματικός ή μιγαδικός χώρος Hilbert και έστω $f : \mathbb{N} \rightarrow \mathbb{H}$ συνάρτηση τέτοια ώστε $\|f(n)\|_{\mathbb{H}} = 1$ για κάθε $n \in \mathbb{N}$. Τότε, το *discrepancy* της f είναι άπειρο.

Αν τώρα, $\mathbb{H}$ πραγματικός χώρος Hilbert, τότε έχουμε:

Πόρισμα 3.1.3. (*Το πρόβλημα discrepancy του Erdős για πραγματικές τιμές*) Κάθε ακολουθία $f(1), f(2), \dots$ με τιμές στο $\{-1, +1\}$ έχει άπειρο *discrepancy*.

3.2 Παραδείγματα

Είναι χρήσιμο να δούμε κάποια σχεδόν αντιπαραδείγματα πάνω σε αυτά τα αποτελέσματα, ώστε να καταδείξουμε την δυσκολία του προβλήματος.

Παράδειγμα 3.2.1. (*Χαρακτήρας Dirichlet*). Έστω $x : \mathbb{N} \rightarrow \mathbb{C}$ όχι-πρωταρχικός χαρακτήρας Dirichlet περιόδου q . Τότε, x είναι πλήρως πολλαπλασιαστική συνάρτηση (δηλαδή, για κάθε $n, m \in \mathbb{N}$ έχουμε $x(mn) = x(m)x(n)$) και ορίζεται ως

$$x(m) = \begin{cases} \zeta_i & , \text{ αν } (m, q) = 1 \\ 0 & , \text{ αν } (m, q) > 1, \end{cases}$$

όπου ζ_i είναι μία $\phi(q)$ -ρίζα της μονάδας. Από τις σχέσεις ορθογωνιότητας των χαρακτήρων Dirichlet (Θεώρημα 1.2.6), έπεται ότι η συνάρτηση x έχει μέση τιμή μηδέν σε οποιοδήποτε διάστημα μήκους q . Άρα, για κάθε ομογενή αριθμητική πρόοδο $\{d, 2d, \dots, nd\}$ και για κάθε $n \in \mathbb{N}$ γράφουμε $n = kq + l$ και έχουμε

$$\begin{aligned} \left| \sum_{j=1}^n x(jd) \right| &= \left| \sum_{j=1}^n x(d)x(j) \right| = |x(d)| \left| \sum_{j=1}^n x(j) \right| \leq \\ &\left| \sum_{j=1}^n x(j) \right| \leq \left| \sum_{j=1}^{kq} x(j) \right| + \left| \sum_{j=1}^l x(j) \right| \leq 0 + q = q. \end{aligned}$$

Δηλαδή, έχει πεπερασμένο Dirichlet. Βέβαια, αυτό δεν αποτελεί αντιπρόδειγμα για το θεώρημα 3.1.2 καθώς ο χαρακτήρας Dirichlet γίνεται μηδέν όταν $(m, q) > 1$, όμως μας δείχνει ότι αναγκαστικά $\|f(n)\| = 1$ για κάθε $n \in \mathbb{N}$ για να ισχύει η εικασία του Erdős.

Παράδειγμα 3.2.2. (παράδειγμα *Borwein-Choi-Coons*). Έστω x_3 όχι πρωταρχικός χαρακτήρας *Dirichlet* περιόδου 3, ο οποίος x_3 παίρνει τιμές:

$$x_3(n) = \begin{cases} +1 & , \text{αν } n \equiv 1 \pmod{3} \\ -1 & , \text{αν } n \equiv 2 \pmod{3} \\ 0 & , \text{αν } n \equiv 0 \pmod{3}. \end{cases}$$

Λόγω του προηγούμενου παραδείγματος ξέρουμε ότι το *discrepancy* του x_3 είναι πεπερασμένο. Κάνουμε την εξής αλλαγή για να έχουμε τις προϋποθέσεις του θεωρήματος 3.1.2(αλλά και του πορίσματος 3.1.3)

$$\tilde{x}_3(p) = \begin{cases} x_3(p) & , \text{αν } p \neq 3 \\ 1 & , \text{αν } p = 3 \end{cases}$$

όπου $\tilde{x}_3 : \mathbb{N} \rightarrow \{-1, +1\}$ παραμένει πλήρως πολλαπλασιαστική.

Έστω $n \in \mathbb{N}$ της μορφής $n = 1 + 3 + \dots + 3^k$, για μεγάλο $k \in \mathbb{N}$. Θεωρούμε το άθροισμα

$$\sum_{j=1}^n \tilde{x}_3(j).$$

Γράφοντας $j = 3^i m$, όπου $(3, m) = 1$ και $i \leq k$, το άθροισμα γίνεται

$$\sum_{j=1}^n \tilde{x}_3(j) = \sum_{i=0}^k \sum_{1 \leq m \leq n/3^i : (m,3)=1} \tilde{x}_3(3^i m).$$

Αρχικά παρατηρούμε ότι

$$(i) \quad \tilde{x}_3(3^i m) = \tilde{x}_3(3^i) \tilde{x}_3(m) = 1 \cdot \tilde{x}_3(m) = \tilde{x}_3(m).$$

(ii) Από το προηγούμενο παράδειγμα γνωρίζουμε ότι ο χαρακτήρας *Dirichlet* x_3 έχει μέση τιμή μηδέν σε κάθε διάστημα μήκους 3. Επιπλέον,

$$\begin{aligned} \lfloor n/3^i \rfloor &= \frac{1}{3^i} + \frac{3}{3^i} + \dots + \frac{3^i}{3^i} + 3 + 3^2 + \dots + 3^{k-i} = \\ &= \sum_{l=0}^i \left(\frac{1}{3}\right)^l + 3(1 + 3 + \dots + 3^{k-i-1}) \end{aligned}$$

προκύπτει δηλαδή ότι $\lfloor n/3^i \rfloor \equiv 1 \pmod{3}$.

Χρησιμοποιώντας τις παρατηρήσεις (i) και (ii) έχουμε ότι:

$$\sum_{1 \leq m \leq n/3^i : (m,3)=1} \tilde{x}_3(3^i m) = 1 \cdot x_3(\lfloor n/3^i \rfloor) = 1,$$

το οποίο ισχύει για κάθε $i = 0, 1, \dots, k$.

Τέλος, επειδή $n = 1 + 3 + \dots + 3^k$, έχουμε ότι $\log n = C + k$ για $C > 1$, άρα αθροίζοντας πάνω από όλα τα $i = 0, 1, \dots, k$ έχουμε:

$$\sum_{j=1}^n \tilde{x}_3(j) = k + 1 \gg \log n,$$

επομένως παίρνοντας *supremum* πάνω από όλα τα $n \in \mathbb{N}$ η συνάρτηση $\tilde{x}_3$ θα έχει άπειρο *discrepancy*.

Δηλαδή, με αυτή την τροποποίηση του παραδείγματος 3.2.1, ώστε να ικανοποιεί τις προϋποθέσεις το θεωρήματος 3.1.2, και μεν δεν αποτελεί αντιπαράδειγμα της εικασίας του Erdős, ωστόσο αν υπολογίσουμε την ποσότητα $\sup_{n \leq N, d \in \mathbb{N}} \left| \sum_{j=1}^n \tilde{x}_3(jd) \right|$ θα δούμε ότι, αρχικά τα πολλαπλάσια του 3 μέχρι το N είναι λιγότερα από τον $\log N$ (για $N \geq 3$) και λόγω της πολλαπλασιαστικότητας της $\tilde{x}_3$ και του ορισμού της, έχουμε:

$$\begin{aligned} \sup_{n \leq N, d \in \mathbb{N}} \left| \sum_{j=1}^n \tilde{x}_3(jd) \right| &= \sup_{n \leq N, d \in \mathbb{N}} |\tilde{x}_3(d)| \left| \sum_{j=1}^n \tilde{x}_3(j) \right| \leq \sup_{n \leq N} \left| \sum_{j=1}^n \tilde{x}_3(j) \right| \leq \\ &\sup_{n \leq N} \left| \sum_{j=3k: 3k < N, k \in \mathbb{N}} \tilde{x}_3(j) \right| + \sup_{n \leq N} \left| \sum_{1 \leq j \leq N: j \neq 3k, k \in \mathbb{N}} \tilde{x}_3(j) \right| \leq \\ &\log N + 2 \ll \log N. \end{aligned}$$

Ενώ αντίστροφα, σύμφωνα με την προηγούμενη ανάλυση,

$$\sup_{n \leq N, d \in \mathbb{N}} \left| \sum_{j=1}^n \tilde{x}_3(jd) \right| \ll \log N.$$

Δηλαδή, η απόκλιση του *discrepancy* της $\tilde{x}_3$ είναι συγκρίσιμο με τον $\log N$.

Άρα, το *discrepancy* της $\tilde{x}_3$ είναι άπειρο αλλά αποκλίνει με αργό ρυθμό (της τάξης του λογαρίθμου) και ενδεχομένως θα μπορούσε να σκεφτεί κάποιος ότι σε κάποιο άλλο παράδειγμα να έχουμε ακόμη πιο αργό ρυθμό, άρα και πεπερασμένο *discrepancy*, το οποίο θα οδηγούσε σε άρνηση της εικασίας του Erdős.

Παράδειγμα 3.2.3. (παράδειγμα Borwein-Choi-Coons, για διανυσματικές τιμές) Έστω $\mathbb{H}$ πραγματικός χώρος Hilbert με ορθοκανονική βάση $\mathcal{I} = (e_0, e_1, \dots)$. Έστω $x_3 = \tilde{x}_3$, όπως στο παράδειγμα 3.2.2 και έστω μια συνάρτηση $f : \mathbb{N} \rightarrow \mathbb{H}$ με τύπο $f(3^a m) = x_3(m) \cdot e_a$, για κάθε $a = 0, 1, \dots$ και $(m, 3) = 1$. Τότε, για κάθε $n \in \mathbb{N}$ ισχύει ότι $\|f(n)\|_{\mathbb{H}} = 1$. Όπως στο προηγούμενο παράδειγμα για $n = 1 + 3 + \dots + 3^k$, τότε

$$\begin{aligned} \sum_{j=1}^n f(j) &= \sum_{a=0}^k \sum_{1 \leq m \leq n/3^a} f(3^a m) = \sum_{a=0}^k \sum_{1 \leq m \leq n/3^a} x_3(m) e_a = \\ &\sum_{a=0}^k e_a \cdot x_3(\lfloor n/3^a \rfloor) = \sum_{a=0}^k 1 \cdot e_a = e_0 + e_1 + \dots + e_k. \end{aligned}$$

Επειδή, $\mathcal{I}$ είναι ορθοκανονική βάση, σύμφωνα με την προηγούμενη σχέση και την εφαρμογή του Πυθαγορείου θεωρήματος έχουμε

$$\left\| \sum_{j=1}^n f(j) \right\|_{\mathbb{H}}^2 = \|e_0 + e_1 + \dots + e_k\|_{\mathbb{H}}^2 = \|e_0\|_{\mathbb{H}}^2 + \|e_1\|_{\mathbb{H}}^2 + \dots + \|e_k\|_{\mathbb{H}}^2 = k + 1,$$

άρα καταλήγουμε στην σχέση

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

Αντίστροφα, έστω $n \in \mathbb{N}$ και έστω $d = 3^l d'$, για $l = 0, 1, \dots$ και $(d', 3) = 1$. Για κάθε $j = 1, 2, \dots, n$ γράφουμε $j = 3^{a_j} \cdot m_j$, όπου $(m_j, 3) = 1$ και επειδή $\mathcal{I}$ είναι ορθοκανονική βάση με την χρήση του Πυθαγορείου θεωρήματος έχουμε

$$\begin{aligned} \left\| \sum_{j=1}^n f(jd) \right\|_{\mathbb{H}}^2 &= \left\| \sum_{j=1}^n f(3^{a_j} \cdot 3^l \cdot d' \cdot m_j) \right\|_{\mathbb{H}}^2 = \left\| \sum_{i \geq 0: 3^i \leq n} e_{i+l} \sum_{m_i \leq n/3^i} x_3(m_i d') \right\|_{\mathbb{H}}^2 = \\ &= \sum_{i \geq 0: 3^i \leq n} \left| \sum_{m_i \leq n/3^i} x_3(m_i d') \right|^2 \cdot \|e_{i+l}\|_{\mathbb{H}}^2 = \sum_{i \geq 0: 3^i \leq n} \left| \sum_{m_i \leq n/3^i} x_3(m_i d') \right|^2. \end{aligned}$$

Τελικά, λόγω πλήρους πολλαπλασιαστικότητας της x_3 και επειδή οι αριθμοί d', m_i έχουν απόλυτη τιμή ίση με ένα, αφού είναι πρώτοι ως προς το 3 και προκύπτει άμεσα

$$\sum_{i \geq 0: 3^i \leq n} \left| \sum_{m_i \leq n/3^i} x_3(m_i d') \right|^2 \leq \sum_{i \geq 0: 3^i \leq n} |x_3(d')|^2 |x_3(m_i)|^2 = \sum_{i \geq 0: 3^i \leq n} 1.$$

Τελικά, έχουμε

$$\left\| \sum_{j=1}^n f(jd) \right\|_{\mathbb{H}} \leq \left(\sum_{i \geq 0: 3^i \leq n} 1 \right)^{1/2} \ll \sqrt{\log n}.$$

Επομένως, το *discrepancy* της f είναι άπειρο και αποκλίνει όπως $\sqrt{\log n}$.

Παράδειγμα 3.2.4. (παράδειγμα *Borwein-Choi-Coons*, για στοχαστικές συναρτήσεις) Έστω (Ω, μ) χώρος πιθανότητας. Θεωρούμε τον χώρο Hilbert $\mathbb{H} = L^2(\Omega, \mu)$ και ορίζουμε την πλήρως πολλαπλασιαστική συνάρτηση $g : \Omega \rightarrow \{-1, +1\}^2$ με τύπο

$$g(\omega)(n) = \begin{cases} x_3(n) & , \text{ αν } (n, 3) = 1 \\ \varepsilon_j & , \text{ αν } n = 3^j m : (m, 3) = 1, \end{cases}$$

όπου x_3 όπως στο παράδειγμα 3.2.2 και $\varepsilon_j \in \{-1, +1\}$ ανεξάρτητες με ίση πιθανότητα.

Δουλεύοντας όπως στο παράδειγμα 3.2.3 έχουμε

$$\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(jd) \right|^2 d\mu(\omega) = \int_{\Omega} \left| \sum_{i \geq 0: 3^i \leq n} \varepsilon_{i+l} \sum_{m_i \leq n/3^i} x_3(m_i d') \right|^2 d\mu(\omega) \leq$$

$$\sum_{i \geq 3^i \leq n} \int_{\Omega} |\varepsilon_{i+l}|^2 \left| \sum_{m_i \leq n/3^i} x_3(m_i d') \right|^2 d\mu(\omega) = \sum_{i \geq 3^i \leq n} 1 \ll \log n,$$

δηλαδή

$$\left(\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(jd) \right|^2 d\mu(\omega) \right)^{1/2} \ll \sqrt{\log n}.$$

Από την άλλη εργαζόμενοι όπως στο παράδειγμα 3.2.2 έχουμε

$$\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) = \int_{\Omega} \left| \sum_{1 \leq j \leq n: (j,3)=1} g(\omega)(j) + \sum_{1 \leq j \leq n: (j,3)>1} g(\omega)(j) \right|^2 d\mu(\omega) \geq$$

$$\int_{\Omega} \left| \frac{k+1}{2} + \sum_{1 \leq j \leq n: (j=3^{i_j} m_j, 3)>1} \varepsilon_{i_j} \right|^2 d\mu(\omega) \geq \frac{k+1}{2} - \mathbb{E} \left| \sum_{1 \leq j \leq n: (j=3^{i_j} m_j, 3)>1} \varepsilon_{i_j} \right|^2,$$

δηλαδή

$$\left(\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(jd) \right|^2 d\mu(\omega) \right)^{1/2} \geq \sqrt{\frac{k+1}{2}} \gg \sqrt{\log n},$$

άρα πάλι έχουμε άπειρο *discrepancy* το οποίο αποκλίνει όπως $\sqrt{\log n}$.

3.3 Σκιαγράφηση της απόδειξης του κεντρικού θεωρήματος

Τα παραπάνω παραδείγματα δείχνουν ότι οι πλήρως πολλαπλασιαστικές συναρτήσεις παίζουν κεντρικό ρόλο στον χειρισμό και τελικά στην απόδειξη του Θεωρήματος 3.1.2. Σε πρώτο στάδιο θα θέλαμε να εμπλέξουμε αυτές τις συναρτήσεις με το θεώρημα 3.1.2 και να προκύψει ένα λογικά ισοδύναμο θεώρημα που θα αφορά τις πλήρως πολλαπλασιαστικές συναρτήσεις.

Αρχικά δίνουμε τον εξής ορισμό για το στοχαστικό στοιχείο.

Ορισμός 3.3.1. (Στοχαστικό στοιχείο) Ορίζουμε ως στοχαστικό στοιχείο, ενός μετρήσιμου χώρου X , να είναι μια τυχαία μεταβλητή g η οποία παίρνει τιμές στον χώρο X . Ισοδύναμα, στοχαστικό στοιχείο είναι μια μετρήσιμη συνάρτηση $g : \Omega \rightarrow X$, όπου (Ω, μ) είναι χώρος πιθανότητας και X ένας μετρήσιμος χώρος.

Επίσης ορίζουμε των χώρο των ακολουθιών από τους φυσικούς στην μοναδιαία σφαίρα, $(S^1)^\mathbb{N} := \{g : \mathbb{N} \rightarrow S^1\}$, τον οποίο εφοδιάζουμε με την παραγόμενη σ-άλγεβρα.

Η ισοδύναμη μορφή του θεωρήματος 3.1.2, με την μορφή πλήρως πολλαπλασιαστικών συναρτήσεων στην γλώσσα των πιθανοτήτων είναι η ακόλουθη:

Θεώρημα 3.3.2. (Ισοδύναμη μορφή του προβλήματος του Erdős για διανυσματικές τιμές) Έστω $g : \mathbb{N} \rightarrow S^1$ στοχαστική και πλήρως πολλαπλασιαστική συνάρτηση που παίρνει τιμές στην μοναδιαία σφαίρα $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. Τότε,

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

Το παραπάνω θεώρημα είναι ισοδύναμο, στην γλώσσα της θεωρίας μέτρου, με την εξής ισοδύναμη μορφή:

Θεώρημα 3.3.3. (Ισοδύναμη μορφή στην θεωρία μέτρου) Έστω (Ω, μ) χώρος πιθανότητας και έστω $g : \Omega \rightarrow (S^1)^\mathbb{N}$ μετρήσιμη πλήρως πολλαπλασιαστική συνάρτηση τέτοια ώστε $g(\omega) \in (S^1)^\mathbb{N}$ πλήρως πολλαπλασιαστική μ -σχεδόν για κάθε $\omega \in \Omega$ (δηλαδή, $g(\omega)(m) = g(\omega)(n)g(\omega)(n)$ για κάθε $n, m \in \mathbb{N}$ και μ -σχεδόν για κάθε $\omega \in \Omega$). Τότε, ισχύει ότι

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

Η ισοδυναμία των θεωρημάτων 3.1.2 και 3.3.2 (ή των θεωρημάτων 3.1.2 και 3.3.3) έρχεται με την χρήση επιχειρημάτων από την ανάλυση Fourier. Αποδεικνύουμε την ισοδυναμία τους στην επόμενη παράγραφο.

Μάλιστα, η στενή σχέση των παραδειγμάτων 3.2.3 και 3.2.4 μπορεί να ερμηνευτεί ως ειδική περίπτωση αυτής της ισοδυναμίας.

Εφόσον, έχουμε την ισοδυναμία των θεωρημάτων για να ολοκληρωθεί η απόδειξη της εικασίας του Erdős αυτό που μένει είναι να αποδείξουμε το θεώρημα 3.3.3 (ή το θεώρημα 3.3.2). Για να συμβεί αυτό θα χρειαστούμε ένα αποτέλεσμα του Terence Tao το οποίο αφορά συσχετισμούς πλήρως πολλαπλασιαστικών συναρτήσεων.

Θεώρημα 3.3.4. (Logarithmically averaged nonasymptotic Elliott conjecture). [6, Theorem 1.3] Έστω a_1, a_2 φυσικοί αριθμοί και b_1, b_2 ακέραιοι τέτοιοι ώστε $a_1 b_2 - a_2 b_1 \neq 0$. Έστω $\varepsilon > 0$, θεωρούμε τους πραγματικούς αριθμούς x, ω και A (όπου ο A είναι αρκούντως μεγάλος, εξαρτώμενος από $\varepsilon, a_1, a_2, b_1, b_2$) τέτοιοι ώστε $x \geq \omega \geq A$ και έστω δύο συναρτήσεις $g_1, g_2 : \mathbb{N} \rightarrow \mathbb{C}$ πολλαπλασιαστικές με $|g_1(n)|, |g_2(n)| \leq 1$ για κάθε φυσικό αριθμό n , οι οποίες ικανοποιούν την σχέση

$$\sum_{p \leq x} \frac{1 - \operatorname{Re} \left(g_1(p) \overline{g_2(p)} p^{-it} \right)}{p} \geq A \quad (3.1)$$

για κάθε χ χαρακτήρα *Dirichlet* περιόδου το πολύ A και για κάθε πραγματικό αριθμό t , με $|t| \leq Ax$. Τότε έχουμε

$$\left| \sum_{x/\omega < n \leq x} \frac{g_1(a_1n + b_1)g_2(a_2n + b_2)}{n} \right| \leq \varepsilon \log \omega. \quad (3.2)$$

Χρησιμοποιώντας αυτό το αποτέλεσμα και ένα επιχείρημα van der Corput, μπορούμε να δείξουμε ότι το μόνο πιθανό αντιπαράδειγμα του θεωρήματος 3.3.2 ή 3.3.3, έρχεται από πλήρως πολλαπλασιαστικές, στοχαστικές συναρτήσεις οι οποίες συμπεριφέρονται σαν τους χαρακτήρες *Dirichlet* (δηλαδή σαν τα παραδείγματα 3.2.1, 3.2.2, 3.3.4).

Ποιό συγκεκριμένα έχουμε την παρακάτω πρόταση.

Πρόταση 3.3.5. (Επιχείρημα van der Corput) Έστω (Ω, μ) χώρος μέτρου και $g : \Omega \rightarrow (S^1)^{\mathbb{N}}$ μετρήσιμη, πλήρως πολλαπλασιαστική μ -σχεδόν παντού, τέτοια ώστε

$$\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \leq C^2, \quad (3.3)$$

για κάποιο πραγματικό αριθμό $C > 0$ και για όλους τους φυσικούς αριθμούς n .

Έστω $\varepsilon > 0$, υποθέτουμε ότι X είναι αρκούντως μεγάλο εξαρτόμενο από τα ε, C . Τότε με πιθανότητα $1 - O(\varepsilon)$ μπορούμε να βρούμε στοχαστικό χαρακτήρα *Dirichlet* $x(\omega)$ με περίοδο $q(\omega) = O_{C,\varepsilon}(1)$ και στοχαστικό πραγματικό αριθμό $t(\omega) = O_{C,\varepsilon}(1)$ τέτοιο ώστε:

$$\sum_{p \leq X} \frac{1 - \operatorname{Re}(g(\omega)(p)x(\omega)(p)p^{-it(\omega)})}{p} \ll_{C,\varepsilon} 1. \quad (3.4)$$

Φυσικά, η υπόθεση αυτής της πρότασης θα σήμαινε ότι αυτή η συνάρτηση $g : \Omega \rightarrow (S^1)^{\mathbb{N}}$ αποτελεί αντιπαράδειγμα για το θεώρημα 3.3.3 και από την στιγμή που το θεώρημα 3.3.3 είναι αληθές η πρόταση 3.3.5 δεν ισχύει.

Ωστόσο, η πρόταση 3.3.5 θα μας είναι χρήσιμη για την απόδειξη του θεωρήματος 3.3.3, καθώς θα ξεκινήσουμε την απόδειξη αυτού με άτοπο, και για αυτό το λόγο η απόδειξη της πρότασης 3.3.5 θα γίνει ξεχωριστά στην παράγραφο 5.

Εφόσον έχουν πραγματοποιηθεί τα προηγούμενα βήματα, μας μένει μόνο να δώσουμε την απόδειξη του θεωρήματος 3.3.3 για πλήρως πολλαπλασιαστικές συναρτήσεις που ικανοποιούν την σχέση (3.4) με μεγάλη πιθανότητα, για μεγάλα X και μικρά ε . Τέτοιες συναρτήσεις μπορούμε να τις δούμε σαν γενίκευση του παραδείγματος των Borwein-Choi-Coons (παράδειγμα 3.2.2). Μάλιστα, χρησιμοποιώντας μια ποιά περίπλοκη ανάλυση από αυτή των παραδειγμάτων 3.2.2 και 3.2.3 αρκεί για να μας δώσει ένα κάτω φράγμα για την ποσότητα $\mathbb{E}|\sum_{j=1}^n \mathbf{g}(j)|^2$ (μάλιστα το φράγμα θα είναι της τάξης του λογαρίθμου, όπως ακριβώς στο παράδειγμα 3.2.3) το οποίο είναι αρκετό για να μας δώσει το άτοπο και τελικά την απόδειξη του θεωρήματος 3.3.3 (ή του θεωρήματος 3.3.2). Επομένως, λόγω της ισοδυναμίας των θεωρημάτων, θα έχει ολοκληρωθεί και η απόδειξη του θεωρήματος 3.1.2 άρα και του πορίσματος 3.1.3. Τα επιχειρήματα για την απόδειξη του θεωρήματος 3.3.3 δίνονται στην παράγραφο 6.

3.4 Συμβολισμοί

Στην συνέχεια θα χρησιμοποιηθούν οι ακόλουθοι συμβολισμοί:

- για τον μέγιστο κοινό διαιρέτη δύο φυσικών αριθμών m, n θα γράφουμε (m, n)
- αν για τους φυσικούς αριθμούς n, d ισχύει ότι ο d διαιρεί τον n , θα γράφουμε $d|n$
- όλα τα γινόμενα και τα αθροίσματα θα είναι πάνω από τους φυσικούς αριθμούς $\mathbb{N} = \{1, 2, \dots\}$, εκτός αν το λέμε ρητά
- για στοχαστικές τυχαίες μεταβλητές θα χρησιμοποιούμε έντονους χαρακτήρες, όπως $\mathbf{g}$, για να ξεχωρίζουν από τις ντετερμινιστικές μεταβλητές, οι οποίες θα συμβολίζονται με κανονικούς χαρακτήρες
- οποτεδήποτε εμφανίζονται πρώτοι αριθμοί αυτοί θα συμβολίζονται πάντα με το γράμμα p , για παράδειγμα $p, p_i, \dots$ και τα λοιπά.
- για την μέση τιμή μιας τυχαίας μεταβλητής $\mathbf{X}$, θα γράφουμε $\mathbb{E}\mathbf{X}$
- με τους συμβολισμούς $X \ll Y$, $Y \gg X$, $X = O(Y)$ θα εννοούμε ότι $|X| \leq C|Y|$, όπου C μια απόλυτη σταθερά. Αν θέλουμε η σταθερά C να εξαρτάται από μία ή και περισσότερες παραμέτρους, τότε θα συμβολίζουμε $X \ll_\varepsilon Y$, $Y \gg_\varepsilon X$, $X = O_\varepsilon(Y)$, όπου σε αυτή την περίπτωση η σταθερά C θα εξαρτάται από την ποσότητα ε .

4 Fourier analytic reduction

Σε αυτή την παράγραφο θα δείξουμε την ισοδυναμία των θεωρημάτων 3.1.2. και 3.3.3.

Θεώρημα. 3.1.2 Έστω $\mathbb{H}$ χώρος Hilbert και $f : \mathbb{N} \rightarrow \mathbb{H}$ με $\|f(n)\|_{\mathbb{H}} = 1$ για κάθε $n \in \mathbb{N}$. Τότε,

$$\sup_{n,d \in \mathbb{N}} \left\| \sum_{j=1}^n f(jd) \right\|_{\mathbb{H}} = \infty.$$

Θεώρημα. 3.3.3 Έστω (Ω, μ) χώρος πιθανότητας και $g : \Omega \rightarrow (S^1)^{\mathbb{N}}$ μετρήσιμη, πλήρως πολλαπλασιαστική μ σχεδόν παντού (δηλαδή, $g(\omega)(mn) = g(\omega)(m)g(\omega)(n)$ για κάθε $n, m \in \mathbb{N}$ και για μ -σχεδόν κάθε $\omega \in \Omega$). Τότε ισχύει ότι

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

Θεώρημα. Τα Θεωρήματα 3.1.2 και 3.3.3 είναι ισοδύναμα.

Απόδειξη. Ξεκινάμε με την εύκολη συνεπαγωγή, δηλαδή θεωρούμε ότι ισχύει το Θεώρημα 3.1.2. και πάμε να αποδείξουμε το θεωρήμα 3.3.3.

Έστω (Ω, μ) και $g : \Omega \rightarrow (S^1)^{\mathbb{N}}$ όπως στο Θεώρημα 3.3.3. Επίσης θεωρούμε τον χώρο Hilbert $\mathbb{H} = L^2(\Omega, \mu)$. Για κάθε $n \in \mathbb{N}$ ορίζουμε $f(n) \in \mathbb{H}$ με τύπο $f(n) : \omega \mapsto g(\omega)(n)$. Επειδή, $g(\omega)(n) \in S^1$ ισχύει ότι

$$\|f(n)\|_{\mathbb{H}}^2 = \int_{\Omega} |g(\omega)(n)|^2 d\mu(\omega) = \int_{\Omega} 1^2 d\mu(\omega) = \mu(\Omega) = 1.$$

Εφόσον ικανοποιούνται οι προϋποθέσεις του Θεωρήματος 3.1.2, ισχύει ότι για κάθε $n \in \mathbb{N}$ αλλά και για κάθε ομογενή αριθμητική πρόοδος $\{d, 2d, \dots, nd\}$ έχουμε:

$$\begin{aligned} \left\| \sum_{j=1}^n f(jd) \right\|_{\mathbb{H}}^2 &= \int_{\Omega} \left| \sum_{j=1}^n g(\omega)(jd) \right|^2 d\mu(\omega) = \int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j)g(\omega)(d) \right|^2 d\mu(\omega) = \\ &= \int_{\Omega} |g(\omega)(d)|^2 \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) = \int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega). \end{aligned}$$

Παίρνοντας τώρα supremum ως προς $n, d \in \mathbb{N}$, από το Θεώρημα 3.1.2 έχουμε:

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

και έτσι έπεται το ζητούμενο.

Έστω τώρα ότι ισχύει το Θεώρημα 3.3.3 και θέλουμε να αποδείξουμε το Θεώρημα 3.1.2.

Με άτοπο, έστω ότι το Θεώρημα 3.1.2 δεν ισχύει, τότε υπάρχει $f : \mathbb{N} \rightarrow \mathbb{H}$ με $\|f(n)\|_{\mathbb{H}} = 1$ για κάθε $n \in \mathbb{N}$ και υπάρχει $C > 0$ τέτοιο ώστε για κάθε ομογενή αριθμητική πρόοδο $\{d, 2d, \dots, nd\}$ να ισχύει

$$\left\| \sum_{j=1}^n f(jd) \right\|_{\mathbb{H}} \leq C. \quad (4.1)$$

Στόχος είναι η κατασκευή μιας συνάρτησης $g : \Omega \rightarrow (S^1)^{\mathbb{N}}$ σε έναν χώρο πιθανότητας (Ω, μ) , η οποία θα είναι μετρήσιμη, πλήρως πολλαπλασιαστική μ -σχεδόν παντού τέτοια ώστε

$$\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \ll_C 1, \forall n \in \mathbb{N}.$$

Για να το πετύχουμε αυτό θα δουλέψουμε σε δύο βήματα:

Βήμα 1: Για κάθε $X \geq 1$ κατασκευάζουμε στοχαστική, πλήρως πολλαπλασιαστική $g_X : \mathbb{N} \rightarrow S^1$ τέτοια ώστε

$$\mathbb{E} \left| \sum_{j=1}^n g_X(j) \right|^2 \ll_C 1, \forall n \leq X.$$

Ισοδύναμα, για κάθε $X \geq 1$ βρίσκουμε χώρο πιθανότητας (Ω_X, μ_X) και κατασκευάζουμε συναρτήσεις $g_X : \Omega_X \rightarrow (S^1)^{\mathbb{N}}$ η οποίες θα είναι μετρήσιμες, πλήρως πολλαπλασιαστικές μ_X -σχεδόν παντού τέτοια ώστε

$$\int_{\Omega_X} \left| \sum_{j=1}^n g_X(\omega)(j) \right|^2 d\mu_X(\omega) \ll_C 1, \forall n \leq X.$$

Έστω $X \geq 1$. Θεωρούμε όλους τους πρώτους αριθμούς $p_1, \dots, p_r$ έως το X . Επίσης, θεωρούμε τον φυσικό αριθμό M τέτοιος ώστε $M \geq X$, αρκούντως μεγάλος και εξαρτώμενος από τους C, X .

Τώρα ορίζουμε δύο συναρτήσεις οι οποίες θα μας χρειαστούν για την συνέχεια:

(i) ορίζουμε την συνάρτηση $F : (\mathbb{Z}/M\mathbb{Z})^r \rightarrow \mathbb{H}$ με τύπο

$$F(a_1(M), \dots, a_r(M)) := f(p_1^{a_1} \cdot \dots \cdot p_r^{a_r}), \text{ όπου } a_1, \dots, a_r \in \{0, 1, \dots, M-1\}.$$

Παρατηρούμε ότι $\|F(\underline{x})\|_{\mathbb{H}} = \|f(n_x)\|_{\mathbb{H}} = 1$, για κάθε $\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r$.

(ii) Ορίζουμε την συνάρτηση $\pi : [1, X] \cap \mathbb{N} \rightarrow (\mathbb{Z}/M\mathbb{Z})^r$ με τύπο

$$\pi(p_1^{a_1} \cdot \dots \cdot p_r^{a_r}) := (a_1, \dots, a_r), \text{ όπου } p_1^{a_1} \cdot \dots \cdot p_r^{a_r} \in [1, X] \cap \mathbb{N}.$$

Παρατηρούμε ότι η συνάρτηση π είναι καλά ορισμένη για $M \geq X$.

Χρησιμοποιώντας την σχέση (4.1), για κάθε $n \leq X$ και βήμα d της μορφής $d = p_1^{a_1} \cdot \dots \cdot p_r^{a_r}$ με $1 \leq a_i \leq M - X$ για κάθε $i \in \{1, \dots, r\}$ καταλήγουμε στην σχέση:

$$\left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}} \leq C.$$

,όπου $\underline{x} = (x_1, \dots, x_r) \in (\mathbb{Z}/M\mathbb{Z})^r$, εκτός από $O_X(M^{r-1})$ στοιχεία από τα συνολικά M^r στοιχεία του συνόλου $(\mathbb{Z}/M\mathbb{Z})^r$.

Πράγματι, θεωρούμε την συνάρτηση $\pi^{-1} : (\mathbb{Z}/M\mathbb{Z})^r \rightarrow [1, X] \cap \mathbb{N}$, με τύπο

$\pi^{-1}(\underline{a}) = \pi^{-1}(a_1, \dots, a_r) = p_1^{a_1} \cdot \dots \cdot p_r^{a_r}$, για την οποία ισχύει ότι:

$$(1) \quad \pi^{-1}(\underline{a} + \underline{b}) = \pi^{-1}((a_1, \dots, a_r) + (b_1, \dots, b_r)) = \pi^{-1}((a_1 + b_1, \dots, a_r + b_r)) = \\ = p_1^{a_1+b_1} \cdot \dots \cdot p_r^{a_r+b_r} = p_1^{a_1} \cdot \dots \cdot p_r^{a_r} \cdot p_1^{b_1} \cdot \dots \cdot p_r^{b_r} = \pi^{-1}(\underline{a}) \cdot \pi^{-1}(\underline{b}).$$

$$(2) \quad f \circ \pi^{-1}(\underline{a}) = f \circ \pi^{-1}((a_1, \dots, a_r)) = f(p_1^{a_1} \cdot \dots \cdot p_r^{a_r}) = F((a_1, \dots, a_r)) = F(\underline{a}).$$

Με βάση τις προηγούμενες δύο παρατηρήσεις έχουμε ότι:

$$F(\underline{x} + \pi(j)) = f(\pi^{-1}(\underline{x} + \pi(j))) = f(\pi^{-1}(\underline{x}) \cdot j) = f(d \cdot j),$$

άρα από την υπόθεση ισχύει ότι:

$$\left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}} = \left\| \sum_{j=1}^n f(jd) \right\|_{\mathbb{H}} \leq C.$$

Επίσης θέλαμε $d = p_1^{a_1} \cdot \dots \cdot p_r^{a_r}$ με $1 \leq a_i \leq M - X$ για κάθε $i \in \{1, \dots, r\}$, έτσι ώστε στο γινόμενο:

$$\pi^{-1}(\underline{x}) \cdot j = d \cdot j = p_1^{a_1} \cdot \dots \cdot p_r^{a_r} \cdot p_1^{b_1} \cdot \dots \cdot p_r^{b_r} = p_1^{a_1+b_1} \cdot \dots \cdot p_r^{a_r+b_r}$$

οι εκθέτες $a_i + b_i \leq M$ για κάθε $i \in \{1, \dots, r\}$, το οποίο ισχύει αφού $n \leq X$, άρα $b_i \leq X$ και $a_i \leq M - X$.

Θεωρούμε το σύνολο $Y = \{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r : \exists i \in \{1, \dots, r\} \text{ με } M - X + 1 \leq x_i \leq M\}$,

τότε για κάθε $x \in Y^c$ ισχύει η προηγούμενη ανίσωση, ενώ για τον πληθύνισμο του Y ισχύει ότι:

$$|Y| = M^r - (M - X)^r = [M - (M - X)][M^{r-1} + M^{r-2}(M - X) + \dots + M(M - X)^{r-2} + (M - X)^{r-1}] <$$

$$X(M^{r-1} + M^{r-2}M + \dots + MM^{r-2} + M^{r-1}) = X(M^{r-1} + M^{r-1} + \dots + M^{r-1} + M^{r-1}) = rXM^{r-1}$$

, όπου r είναι το πλήθος των πρώτων έως τον X .

Επίσης, για $\underline{x} \in Y$ με την χρήση της τριγωνική ανισότητας:

$$\left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}} \leq \sum_{j=1}^n \|F(\underline{x} + \pi(j))\|_{\mathbb{H}} = n \leq X.$$

Με βάση τις προηγούμενες ανισώσεις έχουμε ότι:

$$\begin{aligned}
K &= \frac{1}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}}^2 = \\
&\frac{1}{M^r} \left(\sum_{\underline{x} \in Y^c} \left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}}^2 + \sum_{\underline{x} \in Y} \left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}}^2 \right) = \\
&\leq \frac{1}{M^r} C^2 |Y^c| + \frac{1}{M^r} X^2 |Y| \leq \frac{1}{M^r} C^2 (M - X)^r + \frac{1}{M^r} r X^3 M^{r-1} \leq C^2 + \frac{r X^3}{M}
\end{aligned}$$

και αν επιλέξουμε το $M \geq X^4$, τότε $K \leq C^2 + 1 < 2C^2$, δηλαδή έχουμε:

$$\frac{1}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}}^2 \leq 2C^2. \quad (4.2)$$

Από τον μετασχηματισμό Fourier (διακριτή περίπτωση) έχουμε ότι:

$$F(\underline{x}) = \sum_{\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r} \hat{F}(\underline{\xi}) e^{2\pi i \underline{x} \cdot \underline{\xi} / M},$$

όπου $\underline{x} \cdot \underline{\xi} = x_1 \cdot \xi_1 + \dots + x_r \cdot \xi_r$ το σύνηθες εσωτερικό γινόμενο και για τον μετασχηματισμό Fourier ισχύει $\hat{F} : (\mathbb{Z}/M\mathbb{Z})^r \rightarrow \mathbb{H}$ με τύπο

$$\hat{F}(\underline{\xi}) := \frac{1}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} F(\underline{x}) e^{-2\pi i \underline{x} \cdot \underline{\xi} / M}.$$

Τώρα θεωρούμε την συνάρτηση $T_F : (\mathbb{Z}/M\mathbb{Z})^r \rightarrow [(\mathbb{Z}/M\mathbb{Z})^r \rightarrow \mathbb{H}]$ με τύπο

$(T_F \underline{h})(\underline{x}) = F(\underline{x} + \underline{h})$. Τότε, αν εφαρμόσουμε τον μετασχηματισμό Fourier πάνω σε αυτή την συνάρτηση έχουμε

$$(\hat{T_F \underline{h}})(\underline{\xi}) = \hat{F}(\underline{\xi}) e^{2\pi i \underline{\xi} \cdot \underline{h} / M}.$$

Πράγματι, έστω $\underline{h} \in (\mathbb{Z}/M\mathbb{Z})^r$, τότε η $T_F(\underline{h}) : (\mathbb{Z}/M\mathbb{Z})^r \rightarrow \mathbb{H}$ είναι συνάρτηση και εφαρμόζοντας τον μετασχηματισμό Fourier πάνω της έχουμε ότι για κάθε $\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r$

$$\begin{aligned}
(\hat{T_F \underline{h}})(\underline{\xi}) &= \frac{1}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} T_F(\underline{h})(\underline{x}) e^{-2\pi i \underline{\xi} \cdot \underline{x} / M} = \frac{1}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} F(\underline{x} + \underline{h}) e^{-2\pi i \underline{\xi} \cdot \underline{x} / M} = \\
&\frac{1}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} F(\underline{x} + \underline{h}) e^{-2\pi i \underline{\xi} \cdot \underline{x} / M} e^{-2\pi i \underline{\xi} \cdot \underline{h} / M} e^{2\pi i \underline{\xi} \cdot \underline{h} / M} = \frac{e^{2\pi i \underline{\xi} \cdot \underline{h} / M}}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} F(\underline{x} + \underline{h}) e^{-2\pi i (\underline{x} + \underline{h}) \cdot \underline{\xi} / M}.
\end{aligned}$$

Τώρα κάνοντας την αλλαγή μεταβλητής $\underline{y} = \underline{x} + \underline{h}$, δεν θα αλλάξει κάτι στην άθροιση λόγω της M -περιοδικότητας του συνόλου $(\mathbb{Z}/M\mathbb{Z})^r$ και έτσι έχουμε

$$(T_{F\underline{h}})(\xi) = \frac{e^{2\pi i \xi \underline{h}/M}}{M^r} \sum_{\underline{y} \in (\mathbb{Z}/M\mathbb{Z})^r} F(\underline{y}) e^{-2\pi i \underline{y} \xi/M} = \hat{F}(\underline{\xi}) e^{2\pi i \xi \underline{h}/M}.$$

το οποίο είναι και το ζητούμενο. Χρησιμοποιώντας τώρα αυτή την παρατήρηση έχουμε ότι:

$$\hat{F}(\underline{\xi} + \pi(j)) = (T_{F\pi(j)})(\xi) = \hat{F}(\underline{\xi}) e^{2\pi i \xi \pi(j)/M}. \quad (1)$$

Χρησιμοποιώντας διαδοχικά την ταυτότητα Plancherel (Πρόταση 2.2.3) και την σχέση (1), το αριστερό μέλος της σχέσης (4.2) γίνεται:

$$\begin{aligned} \frac{1}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}}^2 &= \sum_{\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \sum_{j=1}^n \hat{F}(\underline{\xi} + \pi(j)) \right\|_{\mathbb{H}}^2 = \\ &= \sum_{\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \hat{F}(\underline{\xi}) \sum_{j=1}^n e^{2\pi i \xi \pi(j)/M} \right\|_{\mathbb{H}}^2 = \sum_{\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \hat{F}(\underline{\xi}) \right\|_{\mathbb{H}}^2 \left| \sum_{j=1}^n e^{2\pi i \xi \pi(j)/M} \right|^2. \end{aligned}$$

Ένω κάνοντας πάλι χρήση της ταυτότητας Plancherel και επειδή $\|F(\underline{x})\| = 1$, έχουμε:

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

Άρα, η $\|\hat{F}(\underline{\xi})\|_{\mathbb{H}}^2$ είναι κατανομή πιθανότητας των διανυσμάτων $\underline{\xi} = (\xi_1, \dots, \xi_r) \in (\mathbb{Z}/M\mathbb{Z})^r$.

Επομένως ορίζεται ο χώρος πιθανότητας $(\Omega_x, \mu_x) = ((\mathbb{Z}/M\mathbb{Z})^r, \|\hat{F}(\cdot)\|_{\mathbb{H}}^2)$ και τελικά η σχέση (4.2) παίρνει την μορφή:

$$\begin{aligned} \frac{1}{M^r} \sum_{\underline{x} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \sum_{j=1}^n F(\underline{x} + \pi(j)) \right\|_{\mathbb{H}}^2 &= \sum_{\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \hat{F}(\underline{\xi}) \right\|_{\mathbb{H}}^2 \left| \sum_{j=1}^n e^{2\pi i \xi \pi(j)/M} \right|^2 \\ &= \mathbb{E} \left| \sum_{j=1}^n e^{2\pi i \xi \pi(j)/M} \right|^2 \leq 2C^2, \end{aligned} \quad (4.3)$$

η οποία ισχύει για κάθε $n \leq X$.

Θεωρούμε την συνάρτηση $g_x : \Omega_x \rightarrow (S^1)^{\mathbb{N}}$, όπου για δοθέν $\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r$, αρχικά την ορίζουμε πάνω στους πρώτους αριθμούς και έτσι μπορούμε να την επεκτείνουμε σε όλους τους φυσικούς αριθμούς:

Σύμφωνα με τον ορισμό της συνάρτησης π έχουμε $\pi(p_j) = (0, \dots, 0, 1, 0, \dots, 0)$ στην j -θέση και $\underline{\xi} = (\xi_1, \dots, \xi_j, \dots, \xi_r)$, τότε:

$$e^{2\pi i \underline{\xi} \pi(p_j)/M} = e^{2\pi i \xi_j/M}.$$

Με βάση αυτή την παρατήρηση ορίζουμε την συνάρτηση $g_x(\underline{\xi})$ στους πρώτους ως εξής:

$$g_x(\underline{\xi})(p_j) = \begin{cases} e^{2\pi i \xi_j/M} & , \text{για } j = 1, \dots, r \\ 1 & , \text{για } j > r \end{cases}.$$

Τώρα για τυχόν $n \in \mathbb{N}$ γραφουμε την ανάλυση του σε πρώτους παράγοντες

$$n = p_1^{a_1} \cdot \dots \cdot p_r^{a_r} \cdot p_{r+1}^{a_{r+1}} \cdot \dots \cdot p_{r+k}^{a_{r+k}}$$

και για κάθε $\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r$ η συνάρτηση g_x επεκτείνεται σύμφωνα με τον προηγούμενο ορισμό ως:

$$\begin{aligned} g_x(\underline{\xi})(n) &= g_x(\underline{\xi})(p_1^{a_1}) \cdot \dots \cdot g_x(\underline{\xi})(p_r^{a_r}) \cdot 1 \cdot \dots \cdot 1 = \\ &= (g_x(\underline{\xi})(p_1))^{a_1} \cdot \dots \cdot (g_x(\underline{\xi})(p_r))^{a_r} = \\ &= e^{2\pi i (a_1 \cdot \xi_1 + \dots + a_r \cdot \xi_r)/M} \\ &= e^{2\pi i \Pi(n) \underline{\xi}/M}, \end{aligned}$$

όπου η συνάρτηση Π είναι η φυσιολογική επέκταση της συνάρτησης π πάνω σε όλους τους φυσικούς. Δηλαδή, $\Pi|_{[1,X]} = \pi$ και αν για $n \in \mathbb{N}$ αρκετά μεγάλο ώστε να περιέχει στην ανάλυσή του πρώτο μεγαλύτερο του p_r , τότε

$$\Pi(n) = \Pi(p_1^{a_1} \cdot \dots \cdot p_r^{a_r} \cdot p_{r+1}^{a_{r+1}} \cdot \dots \cdot p_{r+k}^{a_{r+k}}) = (a_1, \dots, a_r).$$

Για κάθε $n, m \in \mathbb{N}$ και για κάθε $\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r$ προκύπτει άμεσα από τον ορισμό της και την μοναδικότητα της ανάλυσης σε πρώτους παράγοντες:

$$g_x(\underline{\xi})(nm) = g_x(\underline{\xi})(n) \cdot g_x(\underline{\xi})(m),$$

δηλαδή g_x πλήρως πολλαπλασιαστική για κάθε $\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r$.

Τέλος, σύμφωνα με τον ορισμό της g_x και από την σχέση (4.3) καταλήγουμε στο ότι:

$$\begin{aligned} \mathbb{E} \left| \sum_{j=1}^n g_x(j) \right|^2 &= \sum_{\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \hat{F}(\underline{\xi}) \right\|_{\mathbb{H}}^2 \left| \sum_{j=1}^n g_x(\underline{\xi})(j) \right|^2 = \\ &= \sum_{\underline{\xi} \in (\mathbb{Z}/M\mathbb{Z})^r} \left\| \hat{F}(\underline{\xi}) \right\|_{\mathbb{H}}^2 \left| \sum_{j=1}^n e^{2\pi i \Pi(j) \underline{\xi}/M} \right|^2 = \\ &= \mathbb{E} \left| \sum_{j=1}^n e^{2\pi i \underline{\xi} \Pi(j)/M} \right|^2 \leq 2C^2, \end{aligned}$$

που ισχύει για κάθε φυσικό n με $n \leq X$ και έτσι το πρώτο βήμα έχει πλέον ολοκληρωθεί.

Βήμα 2: Κατασκευή στοχαστικής, πλήρως πολλαπλασιαστικής συνάρτησης $G : \mathbb{N} \rightarrow S^1$ τέτοια ώστε:

$$\sup_{n \in \mathbb{N}} \mathbb{E} \left| \sum_{j=1}^n G(j) \right|^2 \leq 2C^2.$$

Ισοδύναμα, κατασκευή χώρου πιθανότητας (Ω, μ) και κατασκευή μετρήσιμης συνάρτησης $G : \Omega \rightarrow (S^1)^\mathbb{N}$, πλήρως πολλαπλασιαστικής μ -σχεδόν παντού τέτοια ώστε:

$$\sup_{n \in \mathbb{N}} \int_{\Omega} \left| \sum_{j=1}^n G(\omega)(j) \right|^2 d\mu(\omega) \leq 2C^2.$$

Από το Βήμα 1 έχουμε ότι για κάθε $X \geq 1$, υπάρχει χώρος πιθανότητας (Ω_x, μ_x) και συνάρτηση $g_x : \Omega_x \rightarrow (S^1)^\mathbb{N}$ πλήρως πολλαπλασιαστική μ_x -σχεδόν παντού τέτοια ώστε

$$\int_{\Omega_x} \left| \sum_{j=1}^n g_x(\omega)(j) \right|^2 d\mu(\omega) \leq 2C^2, \forall n \leq X. \quad (4.4)$$

Θεωρούμε τον χώρο των πλήρως πολλαπλασιαστικών συναρτήσεων:

$$\mathcal{M} = \{g : \mathbb{N} \rightarrow S^1 \mid g(mn) = g(m)g(n)\}.$$

Τότε, ο χώρος αυτός είναι ισόμορφος με το άπειρο γινόμενο των S^1 , αφού μια πλήρως πολλαπλασιαστική συνάρτηση g καθορίζεται από τις τιμές της στους πρώτους και το σύνολο των πρώτων αριθμών είναι ισοπληθικό με τους φυσικούς, δηλαδή έχουμε

$$\mathcal{M} \simeq (S^1)^\mathbb{N}.$$

Πράγματι, ορίζοντας την συνάρτηση $F : \mathcal{M} \rightarrow (S^1)^\mathbb{N}$ τέτοια ώστε $F(g) = (g(2), g(3), g(5), \dots)$ και θεωρούμε το σύνολο των πρωτων αριθμων $\mathcal{I}$, έτσι έχουμε:

- (i) F 1-1: Έστω $f, g \in \mathcal{M}$ τότε: $F(g) = F(f) \Leftrightarrow (g(2), g(3), \dots) = (f(2), f(3), \dots) \Leftrightarrow g(i) = f(i)$ για κάθε $i \in \mathcal{I} \Leftrightarrow g \equiv f$.
- (ii) F επί: Έστω $x = (x_2, x_3, x_5, \dots) \in (S^1)^\mathbb{N}$. Ορίζουμε την πλήρως πολλαπλασιαστική συνάρτηση $g : \mathbb{N} \rightarrow S^1$ με τις τιμές που παίρνει στους πρώτους να είναι $g(i) = x_i$ για κάθε $i \in \mathcal{I}$ και $g(1) = 1$. Ως πλήρως πολλαπλασιαστική η g καθορίζεται από τις τιμές της στους πρώτους και επομένως είναι καλά ορισμένη, ενώ εξ'ορισμού της F ισχύει ότι $F(g) = x$.
- (iii) F συνεχής: Έστω $(g_n)_{n \in \mathbb{N}}, g \in \mathcal{M}$ με $g_n(i) \rightarrow g(i)$ καθώς $n \rightarrow \infty$ για κάθε $i \in \mathcal{I}$, άρα και για κάθε $j \in \mathbb{N}$ αφού οι συναρτήσεις είναι πλήρως πολλαπλασιαστικές. Τότε εξ'ορισμού της F έχουμε ότι $F(g_n) \rightarrow F(g)$ καθώς $n \rightarrow \infty$ και έτσι η F είναι συνεχής.
- (iv) F^{-1} συνεχής: για δοθέν $x = (x_2, x_3, \dots) \in (S^1)^\mathbb{N}$ ισχύει ότι $F^{-1} = g_x$ τέτοια ώστε $F(g_x) = (g(2), g(3), \dots) = (x_2, x_3, \dots) = x$ και χρησιμοποιώντας την αρχή της μεταφοράς έπεται το ζητούμενο.

Επομένως, ο χώρος $\mathcal{M}$ είναι συμπαγής μετρικός χώρος ως ισόμορφος με τον $(S^1)^\mathbb{N}$.

Για κάθε $X \geq 1$ ορίζουμε το Radon μέτρο πιθανότητας ν_x (δηλαδή, ένα μέτρο ορισμένο στην Borel σ -Αλγεβρα ενός Hausdorff τοπολογικού χώρου, με την ιδιότητα ότι είναι πεπερασμένο στα συμπαγή σύνολα, εξωτερικά κανονικό σε όλα τα Borel σύνολα και εσωτερικά κανονικό στα ανοιχτά σύνολα) ως το pushforward του μέτρου μ_x μέσω της g_x .

Στην συνέχεια θα χρειαστούμε ένα λήμμα από την θεωρία μέτρου.

Λήμμα. Έστω χώρος μέτρου $(X, \mathcal{A}, \mu)$, μετρήσιμος χώρος $(Y, \mathcal{B})$ και μετρήσιμη συνάρτηση $f : X \rightarrow Y$. Ορίζουμε το pushforward μέτρο $\nu = PF(\mu, f)$, δηλαδή $\nu(A) = \mu(f^{-1}(A))$, $\forall A \in \mathcal{B}$. Τότε, για κάθε ολοκληρώσιμη $g : Y \rightarrow \mathbb{C}$ ισχύει ότι $\int_Y g d\nu = \int_X g \circ f d\mu$.

Απόδειξη. Πρώτα θεωρούμε την χαρακτηριστική συνάρτηση $g = 1_E$ για κάποιο Borel σύνολο $E \subset Y$. Παρατηρούμε ότι

$$1_{f^{-1}(E)}(x) = 1 \Leftrightarrow x \in f^{-1}(E) \Leftrightarrow f(x) \in E \Leftrightarrow 1_E(f(x)) = 1. \quad (1)$$

Με βάση τον ορισμό του pushforward μέτρου ν και από την σχέση (1) έχουμε

$$\int_Y g d\nu = \nu(E) = \mu(f^{-1}(E)) = \int_X 1_{f^{-1}(E)} d\mu = \int_X 1_E(f(x)) d\mu(x) = \int_X g \circ f d\mu.$$

Λόγω γραμμικότητας του ολοκληρώματος, για κάθε $g = \sum_{j=1}^n c_j 1_{E_j}$, όπου $n \in \mathbb{N}$, $E_j \subset Y$ Borel σύνολο, συμπεραίνουμε ότι

$$\int_Y g d\nu = \int_X g \circ f d\mu. \quad (2)$$

Στην συνέχεια για τυχαία μη-αρνητική συνάρτηση $g \in L_1(\nu)$, γνωρίζουμε ότι υπάρχει ακολουθία απλών συναρτήσεων $(g_n)_n$ τέτοιες ώστε $g = \sup_n g_n$. Από τον θεώρημα της μονότονης σύγκλισης, με βάση την σχέση (2), έχουμε

$$\int_Y g d\nu = \sup_n \int_Y g_n d\nu = \sup_n \int_X g_n \circ f d\mu = \int_X g \circ f d\mu. \quad (3)$$

Τέλος, για τυχαία $g \in L_1(\nu)$, γράφουμε την g ως άθροισμα $g = g^+ - g^-$. Επειδή, g^+, g^- είναι μη-αρνητικές και ολοκληρώσιμες, από την σχέση (3) έχουμε

$$\int_Y g^+ d\nu = \int_X g^+ \circ f d\mu$$

και

$$\int_Y g^- d\nu = \int_X g^- \circ f d\mu.$$

Με βάση τα προηγούμενα, το ζητούμενο έπεται από την γραμμικότητα του ολοκληρώματος. $\square$

Με βάση το λήμμα ισχύει ότι για κάθε συνεχή $F : \mathcal{M} \rightarrow \mathbb{C}$ έχουμε:

$$\int_{\Omega_x} F(g_x(\omega)) d\mu_x(\omega) = \int_{\mathcal{M}} F(g) d\nu_x(g).$$

Ειδικότερα, για κάθε $n \in \mathbb{N}$ με $n \leq X$, εφόσον η συνάρτηση $F_n : \mathcal{M} \rightarrow \mathbb{C}$ με τύπο

$$F_n(g) = \left| \sum_{j=1}^n g(j) \right|^2 \text{ είναι συνεχής, και χρησιμοποιώντας το βήμα 1 προκύπτει ότι:}$$

$$\int_{\mathcal{M}} F_n(g) d\nu_x(g) = \int_{\Omega_x} F_n \circ g_x(\omega) d\mu_x(\omega) = \int_{\Omega_x} F_n(g_x(\omega)) d\mu_x(\omega) =$$

$$\int_{\Omega_x} \left| \sum_{j=1}^n g_x(\omega)(j) \right|^2 d\mu_x(\omega) \leq 2C^2.$$

Τώρα, επειδή ο χώρος $\mathcal{M}$ είναι συμπαγής μετρικός χώρος ισχύει ότι για κάθε $X \geq 1$ και για κάθε $\varepsilon > 0$, το σύνολο $K = \mathcal{M}$ είναι συμπαγές και $\nu_x(K^c) = \nu_x(\emptyset) = 0 < \varepsilon$. Άρα η συλλογή μέτρων $(\nu_x)_{x \geq 1}$ είναι tight και έτσι μπορούμε να εφαρμόσουμε το θεώρημα του Prokhorov (Θεώρημα 2.1.10) για την συμπαγεία μέτρων πιθανότητας σε συμπαγή μετρικό χώρο. Έτσι έχουμε ότι η συλλογή μέτρων $(\nu_x)_{x \geq 1}$ είναι σχετικά συμπαγής, δηλαδή υπάρχει υπακολουθία $(V_{x_j})_{j \in \mathbb{N}}$ της συλλογής $(\nu_x)_{x \geq 1}$, τέτοια ώστε να συγκλίνει ασθενώς σε ένα ν Radon μέτρο πιθανότητας, καθώς $j \rightarrow \infty$, στον χώρο $\mathcal{M}$ και γράφουμε $\nu_{x_j} \Rightarrow \nu$.

Εξ'ορισμού της ασθενούς σύγκλισης των μέτρων έχουμε ότι για κάθε συνεχή και φραγμένη συνάρτηση $F : \mathcal{M} \rightarrow \mathbb{C}$ ισχύει, για $j \rightarrow \infty$, ότι

$$\int_{\mathcal{M}} F(g) d\nu_{x_j}(g) \rightarrow \int_{\mathcal{M}} F(g) d\nu(g).$$

Ειδικότερα, για κάθε $n \in \mathbb{N}$ για τις συνεχείς και φραγμένες συναρτήσεις $F_n : \mathcal{M} \rightarrow \mathbb{C}$ έχουμε

$$2C^2 \geq \int_{\Omega_{x_j}} \left| \sum_{i=1}^n g_{x_j}(\omega)(i) \right|^2 d\mu_{x_j}(\omega) = \int_{\mathcal{M}} F_n(g) d\nu_{x_j} \rightarrow \int_{\mathcal{M}} F_n(g) d\nu(g) = \int_{\mathcal{M}} \left| \sum_{i=1}^n g(i) \right|^2 d\nu(g),$$

καθώς $j \rightarrow \infty$. Δηλαδή έχουμε:

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

Τέλος, ορίζουμε χώρο πιθανότητας $\Omega = (\mathcal{M}, \nu)$ και την ταυτοτική απεικόνιση $G : \mathcal{M} \rightarrow \mathcal{M}$ με $G = Id_{\mathcal{M}}$, δηλαδή λόγω της ισομορφίας $\mathcal{M} \simeq (S^1)^{\mathbb{N}}$ έχουμε $G : \mathcal{M} \rightarrow (S^1)^{\mathbb{N}}$ και έχουμε ότι για κάθε $n \in \mathbb{N}$

$$\int_{\mathcal{M}} \left| \sum_{j=1}^n G(g)(j) \right|^2 d\nu(g) = \int_{\mathcal{M}} \left| \sum_{j=1}^n g(j) \right|^2 d\nu(g) \leq 2C^2$$

και έτσι ολοκληρώθηκε και το Βήμα 2.

Τελικά, η σχέση

$$\int_{\Omega} \left| \sum_{j=1}^n G(\omega)(j) \right|^2 d\nu(\omega) \leq 2C^2$$

έρχεται σε αντίθεση με το συμπέρασμα του θεωρήματος 3.3.3 και έτσι καταλήγουμε σε άτοπο και η απόδειξη έχει ολοκληρωθεί. $\square$

5 Applying the Elliott – type conjecture

Πρόταση 3.3.5 Έστω (Ω, μ) χώρος μέτρου και $g : \Omega \rightarrow (S^1)^\mathbb{N}$ μετρήσιμη, πλήρως πολλαπλασιαστική μ -σχεδόν παντού, τέτοια ώστε

$$\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \leq C^2, \quad (3.3)$$

για κάποιο πραγματικό αριθμό $C > 0$ και για όλους τους φυσικούς αριθμούς n .

Έστω $\varepsilon > 0$, υποθέτουμε ότι X είναι αρκούντως μεγάλο εξαρτώμενο από τα ε, C . Τότε με πιθανότητα $1 - O(\varepsilon)$ μπορούμε να βρούμε στοχαστικό χαρακτήρα Dirichlet $x(\omega)$ με περίοδο $q(\omega) = O_{C,\varepsilon}(1)$ και στοχαστικό πραγματικό αριθμό $t(\omega) = O_{C,\varepsilon}(X)$ τέτοιο ώστε:

$$\sum_{p \leq X} \frac{1 - \operatorname{Re}(g(\omega)(p)x(\omega)(p)p^{-it(\omega)})}{p} \ll_{C,\varepsilon} 1. \quad (3.4)$$

Απόδειξη. Έστω g, C, ε όπως στην πρόταση. Θεωρούμε $H \geq 1$ μεγάλος φυσικός αριθμός ο οποίος εξαρτάται μόνο από το C, ε (θα διαλεχτεί αργότερα) και έστω X αρκούντως μεγάλο εξαρτώμενο από τα H, ε . Τώρα στην ανίσωση:

$$\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \leq C^2,$$

η οποία ισχύει για κάθε $n \in \mathbb{N}$, αυτή μας δίνει:

$$\frac{1}{n} \int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \leq \frac{1}{n} C^2, \forall n \in \mathbb{N}$$

$$\Rightarrow \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \leq \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} C^2 \leq C^2 \sum_{1 \leq n \leq X} \frac{1}{n} \leq C^2 \int_{t=1}^{t=X} \frac{1}{t} dt = C^2 \log X$$

$$\Leftrightarrow \int_{\Omega} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \leq C^2 \log X. \quad (1)$$

Χρησιμοποιώντας ένα παρόμοιο επιχείρημα (για $X > 1$, ώστε $\log X > 0$), έχουμε για $n' = n + H$, από την σχέση (1):

$$\frac{1}{n} \int_{\Omega} \left| \sum_{j=1}^{n+H} g(\omega)(j) \right|^2 d\mu(\omega) \leq \frac{1}{n} C^2 \forall n \in \mathbb{N} \Rightarrow \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \int_{\Omega} \left| \sum_{j=1}^{n+H} g(\omega)(j) \right|^2 d\mu(\omega) \leq$$

$$C^2 \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \leq C^2 \int_{\sqrt{X}}^X \frac{1}{t} dt = C^2 (\log X - \log \sqrt{X}) \leq C^2 \log X.$$

Τώρα, χρησιμοποιώντας την τριγωνική ανισότητα έχουμε:

$$\begin{aligned} C^2 \log X &\geq \int_{\Omega} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=1}^{n+H} g(\omega)(j) \right|^2 d\mu(\omega) \geq \\ &\int_{\Omega} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=n+1}^{n+H} g(\omega)(j) \right|^2 d\mu(\omega) - \int_{\Omega} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \Leftrightarrow \\ C^2 \log X + \int_{\Omega} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) &\geq \int_{\Omega} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=n+1}^{n+H} g(\omega)(j) \right|^2 d\mu(\omega). \end{aligned}$$

Δηλαδή, έχουμε:

$$\int_{\Omega} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=n+1}^{n+H} g(\omega)(j) \right|^2 d\mu(\omega) \leq 2C^2 \log X.$$

$$\text{Θεωρούμε το σύνολο } A = \left\{ \omega \in \Omega : \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=n+1}^{n+H} g(\omega)(j) \right|^2 \geq 2C^2 \log X \varepsilon^{-1} \right\},$$

τότε χρησιμοποιώντας την ανισότητα Markov έχουμε:

$$\mu(A) \leq \frac{\varepsilon}{2C^2 \log X} \int_{\Omega} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=n+1}^{n+H} g(\omega)(j) \right|^2 d\mu(\omega) \leq \frac{\varepsilon}{2C^2 \log X} 2C^2 \log X = \varepsilon.$$

$$\text{Δηλαδή για το } A^c = \left\{ \omega \in \Omega : \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=n+1}^{n+H} g(\omega)(j) \right|^2 \leq 2C^2 \log X \varepsilon^{-1} \right\},$$

έχουμε $|A^c| \geq 1 - \varepsilon$ και για κάθε $\omega \in A^c$ ισχύει ότι:

$$\sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{j=n+1}^{n+H} g(\omega)(j) \right|^2 \leq 2C^2 \varepsilon^{-1} \log X.$$

Τώρα, με μια αλλαγή μεταβλητής η παραπάνω σχέση γράφεται ως:

$$\sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{h=1}^H g(\omega)(n+h) \right|^2 \leq 2C^2 \varepsilon^{-1} \log X. \quad (5.1)$$

Το αριστερό μέλος της σχέσης (5.1) μπορεί να γραφεί ως:

$$\sum_{h_1, h_2 \in [1, H]} \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h_1)\overline{g(\omega)(n+h_2)}}{n}. \quad (5.2)$$

Πράγματι, επειδή $|g(\omega)(j)| = 1 \ \forall j \in \mathbb{N}$, έχουμε:

$$\begin{aligned} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left| \sum_{h=1}^H g(\omega)(n+h) \right|^2 &= \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} |z_{n,1} + \dots + z_{n,H}|^2 = \\ &= \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} |(a_{n,1} + \dots + a_{n,H}) + i(b_{n,1} + \dots + b_{n,H})|^2 = \\ &= \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} ((a_{n,1} + \dots + a_{n,H})^2 + (b_{n,1} + \dots + b_{n,H})^2) = \\ &= \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left[\sum_{i=1}^H (a_{n,i}^2 + b_{n,i}^2) + 2 \sum_{i=1}^H \sum_{j \neq i, j \in [1, H]} (a_{n,i}a_{n,j} + b_{n,i}b_{n,j}) \right] \\ &= \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} \left[\sum_{i=1}^H 1 + 2 \sum_{i=1}^H \sum_{j \neq i, j \in [1, H]} (a_{n,i}a_{n,j} + b_{n,i}b_{n,j}) \right]. \end{aligned}$$

- Το άθροισμα $\sum_{i=1}^H 1$ αναφέρεται στα $h_1 = h_2$.
- Παρατηρούμε ότι για $z_1, z_2 \in \mathbb{C}$ ισχύει ότι

$$z_1 \bar{z}_2 + z_2 \bar{z}_1 = (a_1 + b_1 i)(a_2 - b_2 i) + (a_2 + b_2 i)(a_1 - b_1 i) = 2(a_1 a_2 + b_1 b_2),$$

δηλαδή αναφέρεται στα $h_1 \neq h_2$.

Από την (5.1) και (5.2) έχουμε

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

Τώρα, γράφουμε την παραπάνω σχέση ως εξής:

$$\sum_{h_1, h_2 \in [1, H]} \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h_1)\overline{g(\omega)(n+h_2)}}{n} = T_d + T_{n-d},$$

όπου T_d ο όρος των διαγώνιων στοιχείων, δηλαδή

$$T_d = \sum_{h_1=h_2 \in [1,H]} \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h_1)\overline{g(\omega)(n+h_2)}}{n} =$$

$$\sum_{h \in [1,H]} \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h)\overline{g(\omega)(n+h)}}{n} = \sum_{h \in [1,H]} \sum_{\sqrt{X} \leq n \leq X} \frac{1}{n}$$

και T_{n-d} ο όρος των μη διαγώνιων στοιχείων, δηλαδή

$$T_{n-d} = \sum_{h_1 \neq h_2 \in [1,H]} \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h_1)\overline{g(\omega)(n+h_2)}}{n}.$$

- Για τον όρο T_d , θεωρούμε τις συναρτήσεις $\phi_n(t) = \frac{1}{n}1_{[n,n+1)}(t)$, $f_n(t) = \frac{1}{t}1_{[n,n+1)}(t)$,

$$\phi(t) = \sum_{n=\sqrt{X}}^X \phi_n(t) \text{ και } f(t) = \sum_{n=\sqrt{X}}^X f_n(t). \text{ Εξ'ορισμού των συναρτήσεων ισχύει ότι}$$

$\phi_n(t) \geq f_n(t) \forall t \in \mathbb{R}$ και έτσι άμεσα έχουμε ότι $\phi(t) \geq f(t) \forall t \in \mathbb{R}$. Προκύπτει ότι:

$$\sum_{\sqrt{X} \leq n \leq X} \frac{1}{n} = \sum_{\sqrt{X} \leq n \leq X} \int_{\mathbb{R}} \phi_n(t) dt = \int_{\mathbb{R}} \sum_{\sqrt{X} \leq n \leq X} \phi_n(t) dt = \int_{\mathbb{R}} \phi(t) dt \geq \int_{\mathbb{R}} f(t) dt =$$

$$\int_{\sqrt{X}}^{X+1} \frac{1}{t} dt = \log(X+1) - \log \sqrt{X} = \log \left(\frac{X+1}{\sqrt{X}} \right) \geq \log \sqrt{X} = \frac{1}{2} \log X,$$

όπου για $X > 1$ ισχύει ότι $X+1 > X \Leftrightarrow \frac{X+1}{\sqrt{X}} > \sqrt{X}$, άρα $\log \left(\frac{X+1}{\sqrt{X}} \right) \geq \log \sqrt{X}$.

$$\text{Έχουμε δηλαδή, } T_d \geq \sum_{h=1}^H \frac{1}{2} \log X = \frac{H}{2} \log X.$$

- Για τον όρο T_{n-d} έχουμε ότι: $T_{n-d} = \sum_{h_1, h_2 \in [1,H]} \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h_1)\overline{g(\omega)(n+h_2)}}{n} - T_d.$

Άρα, $T_{n-d} \in \mathbb{R}$ ως διαφορά πραγματικών αριθμών και επίσης έχουμε:

$$2C^2\varepsilon^{-1} \log X \geq \frac{H}{2} \log X + T_{n-d} \Leftrightarrow |T_{n-d}| \geq \left(\frac{H}{2} - 2C^2\varepsilon^{-1} \right) \log X.$$

Επομένως, για $H \geq 8C^2\varepsilon^{-1}$ (άρα εξαρτάται από τα ε, C) έχουμε ότι $\frac{H}{4} \geq 2C^2\varepsilon^{-1}$ και άρα

$$|T_{n-d}| \geq \frac{1}{4} H \log X.$$

Έτσι,

$$\frac{1}{4}H \log X \leq \left| \sum_{h_1 \neq h_2 \in [1, H]} \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h_1)\overline{g(\omega)(n+h_2)}}{n} \right| \leq \sum_{h_1 \neq h_2 \in [1, H]} \left| \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h_1)\overline{g(\omega)(n+h_2)}}{n} \right|.$$

Χρησιμοποιώντας την αρχή του περιστεριώνα υπάρχουν $h_1(\omega) \neq h_2(\omega)$ (τα οποία είναι στοχαστικά αφού για διαφορετικά ω διαφοροποιείται το $g(\omega)$) τέτοια ώστε:

$$\left| \sum_{\sqrt{X} \leq n \leq X} \frac{g(\omega)(n+h_1(\omega))\overline{g(\omega)(n+h_2(\omega))}}{n} \right| \geq \frac{1/4H \log X}{H^2 - H} = \frac{\log X}{4(H-1)}, \quad (5.3)$$

με το H να έχει εξάρτηση από τα ε και C .

Τώρα στην άρνηση αυτής της πρότασης έχουμε ότι για κάθε χαρακτήρα Dirichlet περιόδου $q = O_{C,\varepsilon}(1)$ και για κάθε $t = O_{C,\varepsilon}(X)$ δεν ισχύει η (3.4) και σύμφωνα με την προηγούμενη ανάλυση ισχύει η σχέση (5.3), η οποία ωστόσο έρχετε σε αντίθεση με την Πρόταση 3.3.4 και έτσι καταλήγουμε σε άτοπο, άρα η απόδειξη έχει ολοκληρωθεί. $\square$

6 A generalised Borwein – Choi – Coons analysis

Θεώρημα 3.3.3 Έστω (Ω, μ) χώρος μέτρου και $g : \Omega \rightarrow (S^1)^\mathbb{N}$ μετρήσιμη, πλήρως πολλαπλασιαστική μ-σχεδόν παντού. Τότε, ισχύει ότι

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

Απόδειξη. Έστω ότι δεν ισχύει, τότε υπάρχει $C > 0$ και υπάρχει $g : \Omega \rightarrow (S^1)^\mathbb{N}$ μετρήσιμη, πλήρως πολλαπλασιαστική μ-σχεδόν παντού τέτοια ώστε $\int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \leq C, \forall n \in \mathbb{N}$.

Στην συνέχεια θα επιλεχθούν με την σειρά οι εξής ποσότητες:

- $0 < \varepsilon < 1/2$, αρκούντως μικρό, εξαρτώμενο από το C .
- $H \in \mathbb{N}$ με $H > 1$, αρκούντως μεγάλο, εξαρτώμενο από τα C, ε .
- $0 < \delta < 1/2$, αρκούντως μικρό, εξαρτώμενο από τα C, ε, H .
- $\kappa \in \mathbb{N}$ με $\kappa \geq 1$, αρκούντως μεγάλο, εξαρτώμενο από τα $C, \varepsilon, H, \delta$.
- $X \in \mathbb{R}$ με $X \geq 1$, αρκούντως μεγάλο, εξαρτώμενο από τα $C, \varepsilon, H, \delta, \kappa$.

Στο μυαλό μας κρατάμε την ιεραρχία:

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

Από την πρόταση (3.3.5) με πιθανότητα $1 - O(\varepsilon)$ υπάρχει χαρακτήρας Dirichlet x , περιόδου $q(\omega) = O_\varepsilon(1)$ και πραγματικός αριθμός $t = O_\varepsilon(X)$ τέτοιος ώστε

$$\sum_{p \leq X} \frac{1 - \operatorname{Re} \left(g(\omega)(p) \overline{x(\omega)(p)} p^{-it(\omega)} \right)}{p} \ll_\varepsilon 1. \quad (6.1)$$

Εάν χρειάζεται μπορούμε να ελλατώσουμε τον χαρακτήρα x και έτσι να θεωρήσουμε ότι ο x είναι primitive.

Στην συνέχεια, είναι βολικό για τους υπολογισμούς να μειώσουμε τον αριθμό t , για αυτό θα χρειαζόμαστε το παρακάτω λήμμα.

Λήμμα. Με πιθανότητα $1 - O(\varepsilon)$ ισχύει ότι :

$$t = O_\varepsilon(X^\delta). \quad (6.2)$$

Απόδειξη. Στην πρόταση 3.3.5 αντικαθιστούμε το X με X^δ και έχουμε ότι με πιθανότητα $1 - O(\varepsilon)$, υπάρχει χαρακτήρας Dirichlet $x'(\omega)$ περιόδου $q'(\omega) = O_\varepsilon(1)$ και πραγματικός αριθμός $t'(\omega) = O_\varepsilon(X^\delta)$ τέτοιος ώστε

$$\sum_{p \leq X^\delta} \frac{1 - \operatorname{Re} g(\omega)(p) \overline{x'(\omega)(p)} p^{-it'(\omega)}}{p} \ll_\varepsilon 1.$$

- Πρώτη περίπτωση: Αν $|t(\omega) - t'(\omega)| < X^\delta$, τότε έχουμε τελειώσει.
- Δεύτερη Περίπτωση: Αν $|t(\omega) - t'(\omega)| \geq X^\delta$, χρησιμοποιούμε το λήμμα 3.1 [8]:

Ορίζουμε την συνάρτηση

$$D(z, w, y) := \left(\sum_{p \leq y} \frac{1 - \operatorname{Re} z(p) \overline{w(p)}}{p} \right)^{1/2},$$

όπου $z := (z(2), z(3), \dots)$, $w := (w(2), w(3), \dots)$, ακολουθίες ορισμένες πάνω στους πρώτους αριθμούς, με $|z(p)|, |w(p)| \leq 1$. Επίσης, ορίζουμε πολλαπλασιασμό αυτών των ακολουθιών με πολλαπλασιασμό κατά συνεταγμένη, δηλαδή $w \cdot z = (w(2)z(2), w(3)z(3), \dots)$.

Το λήμμα 3.1 μας δίνει ότι ισχύει η τριγωνική ανισότητα:

$$D(z_1, w_1, y) + d(z_2, w_2, y) \geq D(z_1 z_2, w_1 w_2, y).$$

Τώρα θεωρούμε τις συναρτήσεις

$$\tilde{x}(\omega)(p) := x(\omega)p^{-it(\omega)}, \tilde{x}'(\omega)(p) := x'(\omega)(p)p^{-it'(\omega)}$$

και εφαρμόζουμε το παραπάνω λήμμα, οπότε έχουμε:

$$\begin{aligned} D(\bar{g}g, \bar{\tilde{x}}\tilde{x}', X^\delta) &= \sum_{p \leq X^\delta} \frac{1 - \operatorname{Re} |g(\omega)(p)|^2 x(\omega)(p) \overline{x'(\omega)(p)} p^{-i(t'(\omega) - t(\omega))}}{p} = \\ &= \sum_{p \leq X^\delta} \frac{1 - \operatorname{Re} x(\omega)(p) \overline{x'(\omega)(p)} p^{-i(t'(\omega) - t(\omega))}}{p} \leq D(\bar{g}, \bar{\tilde{x}}, X^\delta) + D(g, \tilde{x}', X^\delta). \end{aligned}$$

Έχουμε δηλαδή την σχέση:

$$\sum_{p \leq X^\delta} \frac{1 - \operatorname{Re} x(\omega)(p) \overline{x'(\omega)(p)} p^{-i(t'(\omega) - t(\omega))}}{p} \ll_\varepsilon 1. \quad (6.3)$$

Τώρα, χαρακτήρας $x\bar{x}'$ έχει περίοδο $O_\varepsilon(1)$. Εφαρμόζουμε την Vinogradov-Korobov zero-free region για την συνάρτηση $L(\cdot, x\bar{x}')$ [7] και έχουμε ότι $L(\sigma + it, x\bar{x}') \neq 0$ για $|t| \geq 10$ και

$$\sigma \geq 1 - \frac{c_\varepsilon}{(\log |t|)^{2/3} (\log \log |t|)^{1/3}}$$

για κάποια σταθερά c_ε , που εξαρτάται μόνο από το ε . Έπειτα, χρησιμοποιώντας τα επιχειρήματα της Vinogradov-Korobov έχουμε το φράγμα

$$|\log L(\sigma + it, x\bar{x}')| \ll \log^{O(1)} |t|$$

και ελαττώνοντας αν χρειάζεται το c_ε . Τελικά, με τη βοήθεια του λήμματος 2[9] και τα φράγματα $X^\delta \leq |t(\omega)t'(\omega)| \ll_\varepsilon X$ προκύπτει ότι

$$\sum_{\exp((\log X)^{2/3}) \leq p \leq X^\delta} \frac{1 - \operatorname{Re} x(\omega)(p) \overline{x'(\omega)(p)} p^{-i(t'(\omega) - t(\omega))}}{p} \gg \log \log X$$

για X αρκούντως μεγάλο και εξαρτώμενο από ε, δ και επειδή οι προσθεταίοι στην σχέση (6.3) είναι μη αρνητικοί φτάνουμε σε αντίφαση, δηλαδή δεν γίνεται $|t(\omega) - t'(\omega)| \geq X^\delta$, επομένως η απόδειξη του λήμματος έχει ολοκληρωθεί. $\square$

Έστω τώρα ότι υπάρχει μετρήσιμο $A \subset \Omega$ με μέτρο $\mu(A) = 1 - O(\varepsilon)$, δηλαδή με πιθανότητα $1 - O(\varepsilon)$ υπάρχουν τα στοχαστικά x, t τα οποία ικανοποιούν τις σχέσεις (6.1) και (6.2), το οποίο μπορούμε να το κάνουμε εφόσον το ε έχει επιλεγεί μικρό και η πρόταση (3.3.5) ισχύει για κάθε $\varepsilon > 0$.

Το φράγμα στην σχέση (6.1) δείχνει ότι η συνάρτηση $g(\omega)$ συμπεριφέρεται σαν την πλήρως πολλαπλασιαστική συνάρτηση $n \mapsto x(\omega)(n)n^{it(\omega)}$. Έτσι κάνουμε την εξής παραγοντοποίηση:

$$g(\omega)(n) := \tilde{x}(\omega)(n)n^{it(\omega)}h(\omega)(n), \quad (6.4)$$

όπου έχουν οριστεί οι συναρτήσεις:

- (i) $\tilde{x}(\omega)$ έχει νόρμα ίση με 1, είναι πλήρως πολλαπλασιαστική και ως τέτοια καθορίζεται πλήρως από τις τιμές που πέρνει στους πρώτους αριθμούς, επομένως την ορίζουμε ως:

$$\tilde{x}(p) = \begin{cases} x(\omega)(p) & , \text{για } p \nmid q(\omega) \\ g(\omega)(p)p^{-it(\omega)} & , \text{για } p | q(\omega). \end{cases}$$

- (ii) $h(\omega)$ έχει επίσης νόρμα 1, είναι και αυτή πλήρως πολλαπλασιαστική και ορίζεται ως:

$$h(\omega)(p) = \begin{cases} g(\omega)(p)\overline{x(\omega)(p)}p^{-it(\omega)} & , \text{για } p \nmid q(\omega) \\ 1 & , \text{για } p | q(\omega). \end{cases}$$

Με βάση αυτή την παρατήρηση και επειδή $q(\omega) = O_\varepsilon(1)$, μπορούμε να απλοποιήσουμε το φράγμα της σχέσης (6.1) και να πάρουμε την σχέση

$$\left| \sum_{p \leq X} \frac{1 - \operatorname{Re} h(\omega)(p)}{p} \right| \ll_\varepsilon 1. \quad (6.5)$$

Το μοντέλο που έχουμε εδώ είναι να σκεφτούμε ότι $t(\omega) = 0$ και $h(\omega) = 1$, που σε αυτή την περίπτωση από την σχέση (6.4) ισχύει ότι $g(\omega) = \tilde{x}(\omega)$ και έτσι κάποιος θα μπορούσε να παραλείψει τα επόμενα βήματα και να μεταφερθεί αμέσως στην σχέση (6.8). Φυσικά, στην γενική περίπτωση το $t(\omega)$ δεν είναι ταυτοτικά μηδέν (αλλά δεν είναι μεγάλο) και το $h(\omega)$ δεν είναι ταυτοτικά 1 (ωστόσο συμπεριφέρεται σαν μονάδα σύμφωνα με την σχέση (6.5)). Για να φτάσουμε στην σχέση (6.8) θα χρειαστεί να 'αφαιρέσουμε' τους παράγοντες $n^{it(\omega)}$ και $h(\omega)$ από την $g(\omega)$. Στην συνέχεια η σχέση (6.8) περιέχει προσθεταίους τα $\tilde{x}(\omega)$ και με κάποιους υπολογισμούς ακόμα μπορούμε να το απλοποιήσουμε περαιτέρω για να φτάσουμε στην σχέση (6.12) η οποία εμπλέκει μόνο τον χαρακτήρα $x(\omega)$, που θα μπορούσαμε να διαχειριστούμε σχετικά απλά για να φτάσουμε στο άτοπο και τελικά στην απόδειξη του θεωρήματος.

(I) Στόχος τώρα είναι η απαλοιφή του όρου $n^{it(\omega)}$

Από την σχέση (3.3), η οποία ισχύει για κάθε φυσικό αριθμό n , για ένα τυχόν $n \in \mathbb{N}$, έχουμε:

$$C^2 \geq \int_{\Omega} \left| \sum_{j=1}^{n+H'} g(\omega)(j) \right|^2 d\mu(\omega) \geq \int_{\Omega} \left| \sum_{m=1}^{H'} g(\omega)(n+m) \right|^2 d\mu(\omega) - \int_{\Omega} \left| \sum_{j=1}^n g(\omega)(j) \right|^2 d\mu(\omega) \Leftrightarrow$$

$$2C^2 \geq \int_{\Omega} \left| \sum_{m=1}^{H'} g(\omega)(n+m) \right|^2 d\mu(\omega),$$

που ισχύει για κάθε $H' \geq 1$. Άρα, για το επιλεγμένο H ισχύει ότι:

$$2C^2 H \geq \sum_{H < H' \leq 2H} \int_{\Omega} \left| \sum_{m=1}^{H'} g(\omega)(n+m) \right|^2 d\mu(\omega) \Leftrightarrow$$

$$\int_{\Omega} \frac{1}{H} \sum_{H < H' \leq 2H} \left| \sum_{m=1}^{H'} g(\omega)(n+m) \right|^2 d\mu(\omega) \leq 2C^2$$

και επειδή ολοκληρώνουμε μια θετική ποσότητα η ίδια ανίσωση ισχύει και για το ολοκλήρωμα πάνω από το σύνολο $A \subset \Omega$ με $\mu(A) = 1 - O(\varepsilon)$.

Χρησιμοποιώντας τώρα την σχέση $g(\omega)(n) := \tilde{x}(\omega)(n)n^{it(\omega)}h(\omega)(n)$ η παραπάνω ανισότητα γράφεται:

$$\int_{\Omega} \frac{1}{H} \sum_{H < H' \leq 2H} \left| \sum_{m=1}^{H'} \tilde{x}(\omega)(n+m)(n+m)^{it(\omega)}h(\omega)(n+m) \right|^2 d\mu(\omega) \leq 2C^2.$$

- Για $n \geq X^{2\delta}$

Η συνάρτηση $f(z) = (z+n)^{it(\omega)}$ είναι αναλυτική στο μιγαδικό επίπεδο μπορεί να αναπτυχθεί σύμφωνα με το ανάπτυγμα Taylor με κέντρο $z_0 = 0$. Για την ακτίνα σύγκλισης R ισχύει ότι

$R = \lim_{k \rightarrow \infty} \left| \frac{a_k}{a_{k+1}} \right|$, όπου $a_k = \frac{f^{(k)}(z_0)}{k!}$. Επειδή, η k -οστή παράγωγος της f είναι:

$$f^{(k)}(z) = it(\omega)(it(\omega) - 1) \cdot \dots \cdot (it(\omega) - k + 1)(z+n)^{it(\omega)-k}$$

για $z = z_0 = 0$ έχουμε:

$$f^{(k)}(0) = it(\omega)(it(\omega) - 1) \cdot \dots \cdot (it(\omega) - k + 1)n^{it(\omega)-k}.$$

Άρα για την ακτίνα σύγκλισης έχουμε:

$$R = \lim_{k \rightarrow \infty} (k+1) \left| \frac{n}{it(\omega) - k} \right| \leq \lim_{k \rightarrow \infty} \frac{kn + n}{k - t(\omega)} = n.$$

Αντίστροφα, έχουμε

$$R = \lim_{k \rightarrow \infty} (k+1) \left| \frac{n}{it(\omega) - k} \right| \geq \lim_{k \rightarrow \infty} \frac{kn + n}{k + t(\omega)} = n,$$

άρα $R = n$. Επειδή, $n \geq X^{2\delta}$ για αρκετά μεγάλο X , ισχύει ότι $2H < n$ και άρα $m \leq 2H$ ανήκει στον δίσκο σύγκλισης. Έτσι, το ανάπτυγμα Taylor της f για $z = m$ και $z_0 = 0$ είναι

$$(m+n)^{it(\omega)} = n^{it(\omega)} + R_0(m),$$

όπου το $R_0(m)$ είναι το υπόλοιπο και εκτίμηση για αυτό είναι:

$$|R_0(m)| \leq \sum_{j=1}^{\infty} \frac{M \cdot |m-0|^j}{n^j},$$

όπου $M = \max_{w=R} |f(w)|$, ειδικότερα για την f ισχύει ότι $M = 1$ και η παραπάνω σχέση γίνεται:

$$|R_0(m)| \leq \sum_{j=1}^{\infty} \left(\frac{m}{n}\right)^j \leq \sum_{j=1}^{\infty} \left(\frac{2H}{X^{2\delta}}\right)^j \leq \frac{1}{X^\delta} \sum_{j=1}^{\infty} \left(\frac{2H}{X^\delta}\right)^j = \frac{1}{X^\delta} \frac{1}{1 - \frac{2H}{X^\delta}} = O_{H,\delta}(X^{-\delta}).$$

Εδώ η συνεισφορά του σφάλματος είναι αμελητέα, αφού το X έρχεται τελευταίο στην επιλογή, άρα η παραπάνω σχέση(για μεγάλο X) γράφεται ως

$$\int_{\Omega} \frac{1}{H} \sum_{H < H' \leq 2H} \left| \sum_{m=1}^{H'} \tilde{x}(\omega)(n+m)(n)^{it(\omega)} h(\omega)(n+m) \right|^2 d\mu(\omega) \leq C_1,$$

όπου C_1 μια ανεξάρτητη σταθερά. Τέλος βγάζουμε έξω τον παράγοντα $n^{it(\omega)}$, ο οποίος έχει νόρμα 1 καταλήγουμε στο ότι:

$$\int_{\Omega} \frac{1}{H} \sum_{H < H' \leq 2H} \left| \sum_{m=1}^{H'} \tilde{x}(\omega)(n+m) h(\omega)(n+m) \right|^2 d\mu(\omega) \leq C_1.$$

- Για $n < X^{2\delta}$ παίρνουμε κατευθείαν απο την τριγωνική ανισότητα ότι

$$\begin{aligned} \int_{\Omega} \frac{1}{H} \sum_{H < H' \leq 2H} \left| \sum_{m=1}^{H'} g(\omega)(n+m) \right|^2 d\mu(\omega) &\leq \\ \int_{\Omega} \frac{1}{H} \sum_{H < H' \leq 2H} 1H' d\mu(\omega) &\leq \int_{\Omega} \frac{1}{H} 2HH d\mu(\omega) = 2H. \end{aligned}$$

- Αθροίζοντας τώρα πανω από όλα $n \in \mathbb{N}$ με το $1/n^{1+1/\log X}$ (το βάρος τύπου συνάρτησης ζ $\frac{1}{n^{1+1/\log X}}$, θα φανεί χρήσιμο σε επόμενους υπολογισμούς) έχουμε ότι

$$\sum_n \frac{1}{n^{1+1/\log X}} \int_{\Omega} \frac{1}{H} \sum_{H < H' \leq 2H} \left| \sum_{m=1}^{H'} \tilde{x}(\omega)(n+m) h(\omega)(n+m) \right|^2 d\mu(\omega) \leq$$

$$\sum_{n < X^{2\delta}} \frac{2H}{n^{1+1/\log X}} + \sum_{n \geq X^{2\delta}} \frac{1}{n^{1+1/\log X}} \int_{\Omega} \frac{1}{H} \sum_{H \leq H' \leq 2H} \left| \sum_{m=1}^{H'} \tilde{x}(\omega)(n+m)h(\omega)(n+m) \right|^2 d\mu(\omega) \leq$$

$$2H \int_1^{X^{2\delta}} 1/t dt + \sum_{n \geq X^{2\delta}} \frac{C_1}{n^{1+1/\log X}} \leq 4\delta H \log X + \int_{t \geq X^{2\delta}} \frac{C_1}{t^{1+1/\log X}} dt <$$

$$4\delta \frac{1}{\delta} \log X + C_1 \frac{\log X}{X^{2\delta/\log X}} \leq C_2 \log X,$$

όπου C_2 ανεξάρτητη σταθερά. Τέλος, χρησιμοποιώντας την ανισότητα Markov, έχουμε ότι:

$$\mu \left(\left\{ \omega \in A : \frac{1}{H} \sum_{H < H' \leq 2H} \sum_n \frac{|\sum_{m=1}^{H'} \tilde{x}(\omega)(n+m)h(\omega)(n+m)|^2}{n^{1+1/\log X}} \geq \varepsilon^{-1} C_2 \log X \right\} \right) \leq$$

$$\frac{\varepsilon}{C_2 \log X} \int_A \frac{1}{H} \sum_{H < H' \leq 2H} \sum_n \frac{|\sum_{m=1}^{H'} \tilde{x}(\omega)(n+m)h(\omega)(n+m)|^2}{n^{1+1/\log X}} < \varepsilon (1 - O(\varepsilon)) < \varepsilon.$$

Δηλαδή, για το σύνολο B που ορίζεται ως:

$$B = \{ \omega \in A : \frac{1}{H} \sum_{H < H' \leq 2H} \sum_n \frac{|\sum_{m=1}^{H'} \tilde{x}(\omega)(n+m)h(\omega)(n+m)|^2}{n^{1+1/\log X}} \geq \varepsilon^{-1} C_2 \log X \},$$

έχουμε ότι $\mu(B^c) < 1 - O(\varepsilon) - \varepsilon = 1 - O(\varepsilon)$ και $\forall \omega \in B^c$ ισχύει ότι:

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_n \frac{|\sum_{m=1}^{H'} \tilde{x}(\omega)(n+m)h(\omega)(n+m)|^2}{n^{1+1/\log X}} < \varepsilon^{-1} C_2 \log X$$

Παρατήρηση Από εδώ και πέρα τα επιχειρήματα που θα χρησιμοποιηθούν θα είναι ντετερμινιστικά και για μεγαλύτερη ευκολία διαλέγουμε ένα $\omega \in B^c$ και αντί για $x(\omega), h(\omega), q(\omega)$ θα γράφουμε απλώς x, h, q .

(II) Απαλοιφή του h

Για να γίνει αυτό πρέπει να γίνει decouple των $\tilde{x}$ και h στην σχέση

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_n \frac{|\sum_{m=1}^{H'} \tilde{x}(n+m)h(n+m)|^2}{n^{1+1/\log X}} < \varepsilon^{-1} C_2 \log X$$

(για να επιτευχθεί ο διαχωρισμός τους θα εκμεταλευτούμε την σχεδόν περιοδικότητα της $\tilde{x}$ και για αυτό θα ορίσουμε τις παρακάτω κλάσεις). Ορίζουμε τις κλάσεις:

- $a(q^\kappa) \in BAD \Leftrightarrow \exists p|q \text{ και } \exists 1 \leq m \leq 2H \text{ τέτοιο ώστε } p^\kappa | a+m.$
- $a(q^\kappa) \in GOOD \Leftrightarrow a(q^\kappa) \notin BAD,$

όπου $a(q^\kappa) = a \pmod{q^\kappa}.$

Περιοριζόμαστε στους φυσικούς αριθμούς n που ανήκουν στην κλάση $GOOD$, τότε έχουμε την σχέση

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], GOOD} \sum_{n=a(q^\kappa)} \frac{|\sum_{m=1}^{H'} \tilde{x}(n+m)h(n+m)|^2}{n^{1+1/\log X}} < \varepsilon^{-1} C_2 \log X. \quad (1)$$

Χρησιμοποιώντας την ανισότητα Cauchy-Schwarz έχουμε:

$$\begin{aligned} & \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], GOOD} \left| \sum_{n=a(q^\kappa)} \frac{\sum_{m=1}^{H'} \tilde{x}(n+m)h(n+m)}{n^{1+1/\log X}} \right|^2 = \\ & \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], GOOD} \left| \sum_{n=a(q^\kappa)} \frac{\sum_{m=1}^{H'} \tilde{x}(n+m)h(n+m)}{(n^{1+1/\log X})^{1/2}} \cdot \frac{1}{(n^{1+1/\log X})^{1/2}} \right|^2 \leq \\ & \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], GOOD} \left(\sum_{n=a(q^\kappa)} \frac{|\sum_{m=1}^{H'} \tilde{x}(n+m)h(n+m)|^2}{n^{1+1/\log X}} \right) \cdot \left(\sum_{n=a(q^\kappa)} \frac{1}{n^{1+1/\log X}} \right). \end{aligned} \quad (2)$$

- Για το άθροισμα $\sum_{n=a(q^\kappa)} \frac{1}{n^{1+1/\log X}}$, επειδή $n = l \cdot q^\kappa + a$ για κάποιον θετικό ακέραιο l , έχουμε:

$$\begin{aligned} \sum_{n=a(q^\kappa)} \frac{1}{n^{1+1/\log X}} &= \sum_{n=1}^{\infty} \frac{1}{(nq^\kappa + a)^{1+1/\log X}} \leq \\ &\sum_{n=1}^{\infty} \frac{1}{(nq^\kappa)^{1+1/\log X}} \leq \frac{1}{q^\kappa} \sum_{n=1}^{\infty} \frac{1}{n^{1+1/\log X}} \leq \\ &\frac{1}{q^\kappa} \int_{t=1}^{\infty} \frac{1}{t^{1+1/\log X}} dt = \frac{\log X}{q^\kappa}. \end{aligned}$$

Δηλαδή έχουμε την σχέση:

$$\sum_{n=a(q^\kappa)} \frac{1}{n^{1+1/\log X}} \leq \frac{\log X}{q^\kappa}. \quad (3)$$

Επομένως, η σχέση (2), με βάση τις σχέσεις (1) και (3), γίνεται:

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], GOOD} \left(\sum_{n=a(q^\kappa)} \frac{|\sum_{m=1}^{H'} \tilde{x}(n+m)h(n+m)|^2}{n^{1+1/\log X}} \right) \cdot \left(\sum_{n=a(q^\kappa)} \frac{1}{n^{1+1/\log X}} \right) \leq \frac{\varepsilon^{-1} C_2 \log^2 X}{q^\kappa}$$

και τελικά έχουμε

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], GOOD} \left| \sum_{n=a(q^\kappa)} \frac{\sum_{m=1}^{H'} \tilde{x}(n+m)h(n+m)}{n^{1+1/\log X}} \right|^2 < \frac{\varepsilon^{-1} C_2 \log^2 X}{q^\kappa}.$$

Ισχυρισμός. Για $n \in \text{GOOD } a(q^\kappa)$, ισχύει ότι η ποσότητα $\tilde{x}(n+m)$ είναι ανεξάρτητη από την επιλογή του φυσικού n .

Απόδειξη. Έστω $n \in \text{GOOD } a(q^\kappa)$. Από την υπόθεση έχουμε ότι ο μέγιστος κοινός διαιρέτης $(n+m, q^\kappa) = (a+m, q^\kappa)$ δεν διαιρείται από το p^κ για κάθε πρώτο διαιρέτη p του q και έτσι είναι πρώτος παράγοντας του $q^{\kappa-1}$. Επίσης, $\frac{n+m}{(n+m, q^\kappa)} = \frac{n+m}{(a+m, q^\kappa)}$ είναι σχετικά πρώτος ως προς το q . Έτσι για το $\tilde{x}(n+m)$, χρησιμοποιώντας κατά σειρά: τις προηγούμενες δύο παρατηρήσεις, το γεγονός ότι $\tilde{x}$ είναι πλήρως πολλαπλασιαστική, τον ορισμό της $\tilde{x}$ και ότι η x είναι q περιοδική έχουμε ότι:

$$\begin{aligned}\tilde{x}(n+m) &= \tilde{x}\left((n+m, q^\kappa), \frac{n+m}{(n+m, q^\kappa)}\right) = \tilde{x}\left((n+m, q^\kappa) \tilde{x}\left(\frac{n+m}{(n+m, q^\kappa)}\right)\right) = \\ &\tilde{x}\left((a+m, q^\kappa) \tilde{x}\left(\frac{n+m}{(a+m, q^\kappa)}\right)\right) = \tilde{x}\left((a+m, q^\kappa) x\left(\frac{n+m}{(a+m, q^\kappa)}\right)\right) = \\ &\tilde{x}\left((a+m, q^\kappa) x\left(\frac{a+m}{(a+m, q^\kappa)}\right)\right) = \tilde{x}\left((a+m, q^\kappa) \tilde{x}\left(\frac{a+m}{(a+m, q^\kappa)}\right)\right) \\ &= \tilde{x}(a+m).\end{aligned}$$

Εφόσον, η επιλογή του n ήταν τυχαία ισχύει ότι η ποσότητα του $\tilde{x}(n+m)$ είναι ανεξάρτητη του n και πάντα ίση με $\tilde{x}(a+m)$. $\square$

Σύμφωνα με τον ισχυρισμό, η προηγούμενη σχέση με μια εναλλαγή στα αθροίσματα γίνεται:

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], \text{GOOD}} \left| \sum_{m=1}^{H'} \tilde{x}(a+m) \sum_{n=a(q^\kappa)} \frac{h(n+m)}{n^{1+1/\log X}} \right|^2 < \frac{\varepsilon^{-1} C_2 \log^2 X}{q^\kappa}.$$

Με μία αλλαγή μεταβλητής έχουμε ότι

$$\sum_{n=a(q^\kappa)} \frac{h(n+m)}{n^{1+1/\log X}} = \sum_{l=a+m(q^\kappa)} \frac{h(l)}{(l-m)^{1+1/\log X}} = \sum_{n=a+m(q^\kappa)} \frac{h(n)}{(n-m)^{1+1/\log X}}.$$

Θεωρούμε την συνάρτηση

$$f(x) = \frac{1}{(n-m+x)^{1+1/\log X}}, x \in \mathbb{R} - \{m-n\},$$

η οποία είναι παραγωγίσιμη στο πεδίο ορισμού της και η παράγωγός της είναι ίση με

$$f'(x) = -\frac{1+1/\log X}{(n-m+x)^{2+1/\log X}}.$$

Σύμφωνα με το ανάπτυγμα Taylor, η συνάρτηση αναπτύσσεται ως

$$f(x) = T_{n,f,x_0}(x) + R_{n,f,x_0}(x),$$

με το $R_{n,f,x_0}(x)$ να είναι το υπόλοιπο.

Ειδικότερα για $x_0 = m$ και $x = 0$ έχουμε ότι:

$$\frac{1}{(n-m)^{1+1/\log X}} = f(m) + R_{n=0,f,m}$$

$$\frac{1}{(n-m)^{1+1/\log X}} = \frac{1}{n^{1+1/\log X}} + R_{n=0,f,m}.$$

Για το υπόλοιπο σύμφωνα με την μορφή Lagrange ισχύει ότι υπάρχει $\xi \in (0, m)$ τέτοιο ώστε:

$$R_{n=0,f,m}(0) = -\frac{1+1/\log X}{(n-m+\xi)^{2+1/\log X}}(-m) = m \cdot \frac{1+1/\log X}{(n-m+\xi)^{2+1/\log X}}.$$

Αθροίζοντας πάνω από όλα τα $n = a + m(q^\kappa)$ και επειδή $m \leq 2H$ έχουμε:

$$\sum_{n=a+m(q^\kappa)} R_{0,f,m}(0) = \sum_{n=a+m(q^\kappa)} m \cdot \frac{1+1/\log X}{(n-m+\xi)^{2+1/\log X}} \leq m \sum_{n=1}^{\infty} \frac{1}{n^2} < 4m \leq 8H.$$

Επομένως, φτάσαμε στην σχέση για το άθροισμα:

$$\sum_{n=a+m(q^\kappa)} \frac{1}{(n-m)^{1+1/\log X}} \leq \left(\sum_{n=a+m(q^\kappa)} \frac{1}{n^{1+1/\log X}} \right) + 8H.$$

Με αυτή την ανάλυση, τελικά καταλήγουμε:

$$\begin{aligned} \frac{\varepsilon^{-1} C_2 \log^2 X}{q^\kappa} &\geq \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], \text{GOOD}} \left| \sum_{m=1}^{H'} \tilde{x}(a+m) \left(\sum_{n=a+m(q^\kappa)} \frac{h(n)}{n^{1+1/\log X}} + R_{0,f,m} \right) \right|^2 \\ &\geq \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], \text{GOOD}} \left| \sum_{m=1}^{H'} \tilde{x}(a+m) \sum_{n=a+m(q^\kappa)} \frac{h(n)}{n^{1+1/\log X}} \right|^2 - 16H^3 q^\kappa \Leftrightarrow \\ \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], \text{GOOD}} \left| \sum_{m=1}^{H'} \tilde{x}(a+m) \sum_{n=a+m(q^\kappa)} \frac{h(n)}{n^{1+1/\log X}} \right|^2 &\leq \frac{\varepsilon^{-1} C_2 \log^2 X}{q^\kappa} + 16H^3 q^\kappa. \end{aligned}$$

Έτσι για αρκούντως μεγάλο X , ο όρος τάξης $O_H(1)$ μπορεί να απορροφηθεί από τον $\log^2(X)$ και έτσι να φτάσουμε στην σχέση:

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], \text{GOOD}} \left| \sum_{m=1}^{H'} \tilde{x}(a+m) \sum_{n=a+m(q^\kappa)} \frac{h(n)}{n^{1+1/\log X}} \right|^2 < \frac{\varepsilon^{-1} C_3 \log^2 X}{q^\kappa}. \quad (6.6)$$

Στην συνέχεια προσπαθούμε να απλοποιήσουμε το άθροισμα $\sum_{n=a+m(q^k)} \frac{h(n)}{n^{1+1/\log X}}$ και να ολοκληρωθεί η απαλοιφή του όρου $h(n)$.

Παίρνουμε το γινόμενο Euler (Θεώρημα 1.5.4):

$$\sum_n \frac{h(n)}{n^{1+1/\log X}} = \mathfrak{S}$$

το οποίο ορίζεται ως:

$$\mathfrak{S} := \prod_p \left(1 - \frac{h(p)}{p^{1+1/\log X}} \right)^{-1}.$$

Χρησιμοποιώντας την σχέση (6.5) και το θεώρημα Mertens (Θεώρημα 1.6.5) καταλήγουμε στην σχέση:

$$\log X \ll_{\varepsilon} |\mathfrak{S}|.$$

Από την άλλη έχουμε ότι:

$$\begin{aligned} |\mathfrak{S}| &\leq \sum_{n \leq X} \left| \frac{h(n)}{n^{1+1/\log X}} \right| + \sum_{n \geq X} \left| \frac{h(n)}{n^{1+1/\log X}} \right| \\ &\leq \sum_{n \leq X} \frac{1}{n} + \sum_{n \geq X} \frac{1}{n^{1+1/\log X}} \\ &\leq \int_1^X \frac{1}{t} dt + \int_X^\infty \frac{1}{t^{1+1/\log X}} dt \leq \log X + \frac{\log X}{\log X^{1/\log X}} \leq 2 \log X. \end{aligned}$$

Τελικά καταλήγουμε στην σχέση:

$$\log X \ll_{\varepsilon} |\mathfrak{S}| \ll \log X. \quad (6.7)$$

Γενικότερα, εφόσον ο χαρακτήρας Dirichlet είναι πλήρως πολλαπλασιαστική συνάρτηση χρησιμοποιώντας πάλι το γινόμενο Euler έχουμε ότι:

$$\sum_n \frac{x_1(n)h(n)}{n^{1+1/\log X}} = \prod_p \left(1 - \frac{x_1(p)h(p)}{p^{1+1/\log X}} \right)^{-1}$$

το οποίο ισχύει για κάθε χαρακτήρα Dirichlet x_1 .

- Αν ο χαρακτήρας Dirichlet x_1 δεν είναι πρωταρχικός, με περίοδο l τέτοια ώστε $l|q^\kappa$, τότε η L -συνάρτηση $L(s, x_1) := \sum_n \frac{x_1(n)}{n^s}$, είναι αναλυτική κοντά στο 1 και μάλιστα ισχύει ότι:

$$q^\kappa = dl \text{ και } \sum_{n=1}^l x_1(n) = 0 \Rightarrow \left| \sum_{n \leq X} x_1(n) \right| \leq l. \text{ Τέλος, για κάθε } y, x \in \mathbb{N} \text{ έχουμε:}$$

$$\sum_{y \leq n \leq X} \frac{x_1}{n^{1+1/\log X}} \leq \frac{1}{y^{1+1/\log X}} \left| \sum_{y \leq n \leq X} x_1(n) \right| < \left| \sum_{y \leq n \leq X} x_1(n) \right| < l = \frac{q^\kappa}{d}.$$

Δηλαδή δείξαμε ότι:

$$L\left(1 + \frac{1}{\log X}, x_1\right) < \frac{q^\kappa}{d}.$$

Χρησιμοποιώντας αυτήν την παρατήρηση, την ανισότητα Cauchy-Schwarz, το θεώρημα Mertens και την σχέση (6.5) έχουμε ότι:

$$\begin{aligned} \sum_n \frac{x_1(n)h(n)}{n^{1+1/\log X}} &= L\left(1 + \frac{1}{\log X}, x_1\right) \prod_p \left(1 - \frac{h(p)x_1(p)}{p^{1+1/\log X}}\right)^{-1} \left(1 - \frac{x_1(p)}{p^{1+1/\log X}}\right) < \\ \frac{q^\kappa}{d} \prod_p \left(1 - \frac{h(p)x_1(p)}{p^{1+1/\log X}}\right)^{-1} \left(1 - \frac{x_1(p)}{p^{1+1/\log X}}\right) &< \frac{q^\kappa}{d} \exp\left(\sum_p \ln\left(1 - \frac{x_1(p)}{p^{1+1/\log X}}\right) - \ln\left(1 - \frac{h(p)x_1(p)}{p^{1+1/\log X}}\right)\right) \\ &< K \frac{q^\kappa}{d} \exp\left(\sum_{p \leq X} \frac{|1-h(p)|}{p} + \sum_{p > X} \frac{|1-h(p)|}{p^{1+1/\log X}}\right) \leq K' \frac{q^\kappa}{d} \exp\left(\sum_{p \leq X} \frac{|1-h(p)|}{p}\right) = \\ &K' \frac{q^\kappa}{d} \exp\left(\sum_{p \leq X} \frac{((1 - \operatorname{Re}[h(p)])^2 + \operatorname{Im}[h(p)]^2)^{1/2}}{p}\right) = \\ &K' \frac{q^\kappa}{d} \exp\left(\sum_{p \leq X} \frac{(1 - 2\operatorname{Re}[h(p)] + \operatorname{Re}[h(p)]^2 + 1 - \operatorname{Re}[h(p)]^2)^{1/2}}{p}\right) = \\ &K' \frac{q^\kappa}{d} \exp\left(\sum_{p \leq X} \frac{\sqrt{2}(1 - \operatorname{Re}[h(p)])^{1/2}}{p}\right) = K' \frac{q^\kappa}{d} \exp\left(\sum_{p \leq X} \frac{\sqrt{2}}{\sqrt{p}} \frac{(1 - \operatorname{Re}[h(p)])^{1/2}}{\sqrt{p}}\right) \leq \\ &K' \frac{q^\kappa}{d} \exp\left(\sum_{p \leq X} \left(\frac{2}{p}\right)^{1/2} \left(\sum_{p \leq X} \frac{1 - \operatorname{Re}[h(p)]}{p}\right)^{1/2}\right) = \\ &K' \frac{q^\kappa}{d} \exp\left(\left[2\left(\log \log X + A + O\left(\frac{1}{\log X}\right)\right) \left(\sum_{p \leq X} \frac{1 - \operatorname{Re}[h(p)]}{p}\right)\right]^{1/2}\right) \leq \\ &K' \frac{q^\kappa}{d} \exp\left(\left[2\left(\log \log X + A + O\left(\frac{1}{\log X}\right)\right) C_\varepsilon\right]^{1/2}\right). \end{aligned}$$

- Τώρα για πρωταρχικούς χαρακτήρες Dirichlet x_0 , περιόδου r , με $r|q^\kappa$, χρησιμοποιώντας τον ορισμό του γινομένου Euler, τον ορισμό του πρωταρχικού χαρακτήρα Dirichlet, τον ορισμό της συνάρτησης h , έχουμε ότι:

$$\begin{aligned} \sum_n \frac{x_0 h(p)}{n^{1+1/\log X}} &= \prod_{p|r} \left(1 - \frac{h(p)}{p^{1+1/\log X}}\right)^{-1} = \\ &= \mathfrak{G} \prod_{p|r} \left(1 - \frac{1}{p^{1+1/\log X}}\right). \end{aligned} \quad (1)$$

Στην συνέχεια, θεωρούμε την συνάρτηση $f : \mathbb{R} \rightarrow \mathbb{R}$ με τύπο $f(t) = 1 - \frac{1}{p^{1+t}}$. Τότε, η f είναι παραγωγίσιμη και $f'(t) = \frac{1}{p} \frac{1}{p^{1+t}}$. Από το ανάπτυγμα Taylor έχουμε

$$f(x) = T_{n,f,x_0}(x) + R_{n,f,x_0}(x), \quad (2)$$

όπου $T_{n,f,x_0}(x) = \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k$ και $R_{n,f,x_0}(x)$ το υπόλοιπο. Ειδικότερα, για $x = 1/\log X$, $x_0 = 0$, $n = 0$ έχουμε από το υπόλοιπο Lagrange ότι υπάρχει $\xi \in (0, 1/\log X)$ τέτοιο ώστε

$$R_{0,f,0}(1/\log X) = \frac{f'(\xi)}{0!} (1/\log X - 0) = \frac{1}{p} \frac{1}{\log X} \frac{\xi}{p^{\xi+1}} < \frac{1}{p} \frac{1}{\log X},$$

ενώ $f(1/\log X) = 1 - \frac{1}{p^{1+1/\log X}}$ και $T_{0,f,0}(1/\log X) = 1 - \frac{1}{p}$. Έτσι η σχέση (2) γίνεται:

$$1 - \frac{1}{p^{1+1/\log X}} = 1 - \frac{1}{p} + R_{0,f,0}(1/\log X), \quad (3)$$

όπου $|R_{0,f,0}(1/\log X)| < \frac{1}{p} \frac{1}{\log X}$. Έτσι, η σχέση (1) με βάση την σχέση (3) γίνεται:

$$\mathfrak{G} \left(1 + O\left(\frac{1}{\log X}\right)\right) \prod_{p|r} \left(1 - \frac{1}{p}\right).$$

Τελικά, χρησιμοποιώντας την σχέση (6.7) και ότι $\prod_{p|r} \left(1 - \frac{1}{p}\right) = \frac{\phi(r)}{r}$ (Θεώρημα 1.1.3), έχουμε

ότι:

$$\frac{\phi(r)}{r} \mathfrak{G} + O_\varepsilon(1),$$

όπου κάθε πρώτος παράγοντας της περιόδου r διαιρεί και το q , άρα είναι μεγέθους το πολύ $O_\varepsilon(1)$, εφόσον για τον αριθμό q ισχύει ότι $q = O_\varepsilon(1)$.

Κρατάμε την σχέση :

$$\sum_n \frac{x_0 h(p)}{n^{1+1/\log X}} = \frac{\phi(r)}{r} \mathfrak{G} + O_\varepsilon(1).$$

Τώρα, είναι γνωστο ότι δεδομένης της περιόδου r υπάρχουν ακριβώς $\phi(r)$ το πλήθος χαρακτήρες Dirichlet (Πρόταση 1.2.4.) και από τις σχέσεις ορθογωνιότητας (θεώρημα 1.2.6.) έχουμε ότι:
 $\Gamma_a n \equiv 1 \pmod r$

$$x_0(n) + x_1(n) + \dots + x_{\phi(r)-1}(n) = \phi(r),$$

ενώ για $n \not\equiv 1 \pmod r$

$$x_0(n) + x_1(n) + \dots + x_{\phi(r)-1}(n) = 0.$$

Με βάση τα παραπάνω παρατηρούμε ότι:

$$\begin{aligned} \sum_{n \equiv 1 \pmod r} \frac{h(n)}{n^{1+1/\log X}} &= \\ \sum_{n \not\equiv 1 \pmod r} \frac{h(n)}{n^{1+1/\log X}} \frac{(x_0(n) + \dots + x_{\phi(r)-1}(n))}{\phi(r)} + \sum_{n \equiv 1 \pmod r} \frac{h(n)}{n^{1+1/\log X}} \frac{(x_0(n) + \dots + x_{\phi(r)-1}(n))}{\phi(r)} &= \\ \sum_n \frac{h(n)}{n^{1+1/\log X}} \frac{(x_0(n) + \dots + x_{\phi(r)-1}(n))}{\phi(r)}. \end{aligned}$$

Αν τώρα $n \equiv b \pmod r$, όπου $(b, r) = 1$ (δηλαδή b όχι απαραίτητα ίσο με 1), τότε λόγω της πλήρους πολλαπλασιαστικότητας της h έχουμε:

$$\begin{aligned} \sum_{n \equiv b \pmod r} \frac{h(n)}{n^{1+1/\log X}} &= \sum_{n \equiv 1 \pmod r} \frac{h(bn)}{(bn)^{1+1/\log X}} = \frac{h(b)}{b^{1+1/\log X}} \sum_{n \equiv 1 \pmod r} \frac{h(n)}{n^{1+1/\log X}} = \\ \frac{h(b)}{b^{1+1/\log X}} \sum_n \frac{h(n)}{n^{1+1/\log X}} \frac{(x_0(n) + \dots + x_{\phi(r)-1}(n))}{\phi(r)}. \end{aligned}$$

Έτσι, τώρα για κάθε πρωταρχική κλάση υπολοίπων (δηλαδή, για κάθε κλάση υπολοίπων b με $(b, r) = 1$) έχουμε ότι:

$$\begin{aligned} \sum_{n \equiv b \pmod r} \frac{h(n)}{n^{1+1/\log X}} &= \frac{h(b)}{b^{1+1/\log X}} \sum_n \frac{h(n)}{n^{1+1/\log X}} \frac{(x_0(n) + \dots + x_{\phi(r)-1}(n))}{\phi(r)} = \\ \frac{h(b)}{b^{1+1/\log X}} \sum_{j=0}^{\phi(r)-1} \sum_n \frac{h(n)}{n^{1+1/\log X}} \frac{x_j(n)}{\phi(r)} &= \\ \frac{h(b)}{b^{1+1/\log X}} \sum_n \frac{h(n)}{n^{1+1/\log X}} \frac{x_0(n)}{\phi(r)} + \frac{h(b)}{b^{1+1/\log X}} \sum_{j=1}^{\phi(r)-1} \sum_n \frac{h(n)}{n^{1+1/\log X}} \frac{x_j(n)}{\phi(r)} &= \\ \frac{h(b)}{b^{1+1/\log X}} \left(\frac{1}{r} \mathfrak{S} + O_\varepsilon(1) + \frac{\phi(r)-1}{\phi(r)} K' \frac{q^\kappa}{d} \exp \left(\left(2 \left[\log \log X + A + O \left(\frac{1}{\log X} \right) \right] C_\varepsilon \right)^{1/2} \right) \right) &= \\ C_{(b)} \left(\frac{1}{r} \mathfrak{S} + O_\varepsilon(1) + O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2})) \right), \end{aligned}$$

όπου $|C_{(b)}| \leq 1$. Δηλαδή, έχουμε την σχέση:

$$\sum_{n \equiv b \pmod r} \frac{h(n)}{n^{1+1/\log X}} = \frac{1}{r} \mathfrak{S} + O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2})).$$

Για τις μη πρωταρχικές κλάσεις (δηλαδή, $(b, r) > 1$) γράφουμε $r = (b, r)r'$ και $b = (b, r)b'$. Τότε, $(b', r') = 1$ και σύμφωνα με τα προηγούμενα

$$\sum_{n \equiv b' \pmod{r'}} \frac{h(n)}{n^{1+1/\log X}} = \frac{1}{r'} \mathfrak{S} + O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2})).$$

Αν $n \equiv b \pmod r$, τότε $n = k(b, r)r' + (b, r)b' = (b, r)(kr' + b')$, για κάποιο ακέραιο k . Επειδή, $h((b, r)) = 1$ έχουμε το άθροισμα

$$\begin{aligned} & \sum_{k=1}^{\infty} \frac{h((b, r))h(kr' + b')}{(b, r)^{1+1/\log X} (kr' + b')^{1+1/\log X}} = \\ & = \frac{1}{(b, r)^{1+1/\log X}} \sum_{n \equiv b' \pmod{r'}} \frac{h(n)}{n^{1+1/\log X}} = \\ & = \frac{1}{(b, r)^{1+1/\log X}} \left[\frac{1}{r'} \mathfrak{S} + O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2})) \right]. \end{aligned}$$

Τέλος, χρησιμοποιώντας την σχέση (6.7) καταλήγουμε στην ισότητα:

$$\sum_{n \equiv b \pmod r} \frac{h(n)}{n^{1+1/\log X}} = \frac{1}{r} \mathfrak{S} + O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2})),$$

η οποία ισχύει για όλες τις κλάσεις υπολοίπων, πρωταρχικές και μη.

Γυρίζοντας τώρα στην σχέση (6.6) έχουμε ότι:

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa], GOOD} \left| \sum_{m=1}^{H'} \tilde{x}(a+m) \left(\frac{1}{r} \mathfrak{S} + O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2})) \right) \right|^2 < \frac{\varepsilon^{-1} C_3 \log^2 X}{q^\kappa}.$$

Τώρα, η συνεισφορά του όρου $O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2}))$ μπορεί να δειχθεί, με την βοήθεια της σχέσης (6.7) και για αρκούντως μεγάλο X , ότι είναι το πολύ $c_\varepsilon \log^2 X / q^\kappa$.

Πράγματι, για X τέτοιο ώστε $\log X / q^{2\kappa} > 1$ έχουμε ότι:

$$O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2})) =$$

$$\begin{aligned} \frac{\phi(r)-1}{\phi(r)} K' \frac{q^\kappa}{d} \exp \left(\left(2 \left[\log \log X + A + O \left(\frac{1}{\log X} \right) \right] C_\varepsilon \right)^{1/2} \right) < \\ K' q^\kappa \exp((4 \log \log X C_\varepsilon)^{1/2}) < K' q^\kappa (\exp(\log \log X))^{2\sqrt{C_\varepsilon}} = K' q^\kappa (\log X)^{2\sqrt{C_\varepsilon}} < \\ K' q^\kappa |\mathfrak{G}|^{2\sqrt{C_\varepsilon}} < c_\varepsilon K' q^\kappa \log X < c_\varepsilon K' q^\kappa \frac{\log^2 X}{q^{2\kappa}} = K' c_\varepsilon \log^2 X / q^\kappa. \end{aligned}$$

Τέλος, χρησιμοποιώντας πάλι την σχέση (6.7) έχουμε ότι $|\mathfrak{G}| < \log X$ και έτσι ο όρος $\frac{1}{r} \mathfrak{G} + O_{q,k}(\exp(O_\varepsilon(\log \log X)^{1/2}))$ μπορεί να βγει από το άθροισμα και εφόσον είναι ανεξάρτητος από τις μεταβλητές m, a, H' και λόγω των προηγούμενων δύο ανισωτικών τους σχέσεων, καταλήγουμε στην σχέση:

$$\frac{1}{q^\kappa} \sum_{a \in [1, q^\kappa], \text{GOOD}} \frac{1}{H} \sum_{H < H' \leq 2H} \left| \sum_{m=1}^{H'} \tilde{x}(a+m) \right|^2 \leq K'' c_\varepsilon, \quad (6.8)$$

η οποία έχει εξάρτηση μόνο από την ποσότητα ε .

Τελικός μας στόχος είναι να βρούμε κάτω φράγμα που θα έρχεται σε αντίθεση με την σχέση (6.8) και έτσι θα φτάσουμε σε άτοπο και άρα στην απόδειξη του θεωρήματος. Όπως αναφέρθηκε παραπάνω, αυτή θα είναι μία πιο περίπλοκη διαδικασία σε σχέση με τα παραδείγματα 3.2.2, 3.2.3, 3.2.4, καθώς η πλήρης ορθογωνιότητα έχει αντικατασταθεί από μία 'σχεδόν' ορθογωνιότητα.

Διακρίνουμε περιπτώσεις για την ποσότητα q :

Αν το $q = 1$, τότε εξ'ορισμού της συνάρτησης $\tilde{x}$ ισχύει ότι $\tilde{x} \equiv 1$ και έτσι η σχέση (6.8) γίνεται:

$$K'' c_\varepsilon \geq \frac{1}{H} \sum_{H < H' \leq 2H} H'^2 \geq \frac{1}{H} \sum_{H < H' \leq 2H} H^2 = \frac{1}{H} H H^2 = H^2,$$

το οποίο είναι άτοπο αφού η επιλογή του H έρχεται μετά την επιλογή του ε , άρα μπορεί να επιλεγεί αρκετά μεγάλο για να φτάσουμε σε άτοπο.

Αν το $q > 1$, ώστε ο χαρακτήρας Dirichlet δεν είναι πρωταρχικός και μπορούμε να γράψουμε την σχέση (6.8) ως:

$$\frac{1}{H} \sum_{H < H' \leq 2H} \sum_{m_1, m_2 \in [1, H']} \sum_{a \in [1, q^\kappa], \text{GOOD}} \tilde{x}(a+m_1) \overline{\tilde{x}(a+m_2)} \leq K'' c_\varepsilon q^\kappa.$$

Τώρα, ορίζουμε $d_1 := (a+m_1, q^\kappa)$ και $d_2 := (a+m_2, q^\kappa)$ και παρατηρούμε ότι:

- (i) $d_1, d_2 | q^{\kappa-1}$.
- (ii) $\left(\frac{a+m_i}{d_i}, q \right)$ για $i \in \{1, 2\}$.

Πράγματι, για το (i) αρκεί να το δείξουμε για το d_1 , τότε όμοια αποδεικνύεται και για το d_2 . Από την ανάλυση των $q, a + m_1$ σε πρώτους παράγοντες έχουμε:

- $q = p_1^{l_1} \cdot \dots \cdot p_{n_1}^{l_{n_1}} \cdot A$, όπου $(A, p_1^{l_1} \cdot \dots \cdot p_{n_1}^{l_{n_1}}) = 1$.
- $a + m_1 = p_1^{s_1} \cdot \dots \cdot p_{n_1}^{s_{n_1}} \cdot B$, όπου $(B, p_1^{s_1} \cdot \dots \cdot p_{n_1}^{s_{n_1}}) = 1$.

Εφόσον, $a \in GOOD$ ισχύει ότι $s_1, \dots, s_{n_1} \leq \kappa - 1$ (αφού για κάθε $p|q$ και για κάθε m ισχύει $p^\kappa \nmid a + m$). Άρα, $d_1 = \prod_{i=1}^{n_1} p_i^{\min(kl_i, s_i)}$ και $\min(kl_i, s_i) \leq \kappa - 1$. Τέλος,

$$q^{\kappa-1} = p_1^{(\kappa-1)l_1} \cdot \dots \cdot p_{n_1}^{(\kappa-1)l_{n_1}} \cdot A^{\kappa-1} \text{ και επειδή } l_i \geq 1 \text{ έχουμε } (\kappa-1)l_i \geq \kappa-1 \text{ και έτσι } d_1 | q^{\kappa-1}.$$

Για το (ii), πάλι αρκεί να το δείξουμε για m_1, d_1 και όμοια προκύπτει για m_2, d_2 . Αναλύουμε τα $q, a + m_1$ σε πρώτους παράγοντες:

- $q = p_1^{l_1} \cdot \dots \cdot p_{n_1}^{l_{n_1}} \cdot A$, όπου $(A, p_1^{l_1} \cdot \dots \cdot p_{n_1}^{l_{n_1}}) = 1$.
- $a + m_1 = p_1^{s_1} \cdot \dots \cdot p_{n_1}^{s_{n_1}} \cdot B$, όπου $(B, p_1^{s_1} \cdot \dots \cdot p_{n_1}^{s_{n_1}}) = 1$.

και επειδή $p_i^\kappa \nmid a + m_1$, έχουμε ότι $s_i \leq \kappa - 1$. Άρα $d_1 = p_1^{m_1} \cdot \dots \cdot p_{n_1}^{m_{n_1}}$, με $m_i = \min\{s_i, l_i \kappa\}$, άρα $m_i \leq s_i \leq \kappa - 1$. Αν τώρα αναλύσουμε το $\frac{a+m_1}{d_1}$ σε πρώτους παράγοντες έχουμε:

$$\bullet \frac{a+m_1}{d_1} = \frac{p_1^{s_1} \cdot \dots \cdot p_{n_1}^{s_{n_1}} \cdot B}{p_1^{m_1} \cdot \dots \cdot p_{n_1}^{m_{n_1}}} = p_1^{s_1-m_1} \cdot \dots \cdot p_{n_1}^{s_{n_1}-m_{n_1}} \cdot B.$$

Έστω ότι $\left(\frac{a+m_1}{d_1}, q\right) > 1$, τότε υπάρχει τουλάχιστον ένα $s_i - m_i \geq 1$. Τότε,

αν $d = \left(\frac{a+m_1}{d_1}, q^\kappa\right)$, έχουμε ότι $d | \frac{a+m_1}{d_1} \Rightarrow \frac{a+m_1}{d_1} = rd = p_i r' d$, όπου (p_i, r') όχι απαραίτητα ίσος με 1, για κάποιο $i \in \{1, \dots, n_1\}$.

$$\text{Άρα, } d = (r' p_1^{m_1} \cdot \dots \cdot p_i^{m_i+1} \cdot \dots \cdot p_{n_1}^{m_{n_1}}, p_1^{l_1 \kappa} \cdot \dots \cdot p_{n_1}^{l_{n_1} \kappa} \cdot A^\kappa).$$

Επειδή, $m_i \leq \kappa - 1$ και $l_i \geq 1$, ισχύει ότι $m_i + 1 \leq \kappa \leq \kappa l_i$. Δηλαδή,

$$d > dp_i > d, \text{ το οποίο είναι άτοπο και έτσι } \left(\frac{a+m_1}{d_1}, q\right) = 1.$$

Με βάση την παραπάνω παρατήρηση, τον ορισμό της $\tilde{x}$ και το γεγονός ότι είναι πλήρως πολλαπλασιαστική, έχουμε για $i \in \{1, 2\}$:

$$\tilde{x}(a + m_i) = \tilde{x}\left(d_i \frac{a + m_i}{d_i}\right) = \tilde{x}(d_i) \tilde{x}\left(\frac{a + m_i}{d_i}\right) = \tilde{x}(d_i) x\left(\frac{a + m_i}{d_i}\right).$$

Άρα, η προηγούμενη σχέση μπορεί να γραφεί ως:

$$\sum_{d_1, d_2 | q^{\kappa-1}} \tilde{x}(d_1) \overline{\tilde{x}(d_2)} \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{m_1, m_2 \in [1, H']} \sum_{a \in A} x\left(\frac{a + m_1}{d_1}\right) \overline{x\left(\frac{a + m_2}{d_2}\right)} \leq K'' c_\varepsilon q^\kappa, \quad (6.9)$$

όπου $a \in A \Leftrightarrow a \in [1, q^\kappa], a \in GOOD : (a + m_1, q^\kappa) = d_1, (a + m_2, q^\kappa) = d_2$.

Τώρα, ξαναγυρίζουμε πίσω στην κλάση BAD και θέλουμε να δείξουμε ότι έχει αμελητέα το πλήθος στοιχείων.

Πράγματι, αν $a \in BAD$ τότε εξ'ορισμού αυτής της κλάσης $\exists p|q \exists 1 \leq m \leq 2H$ τέτοια ώστε $p^\kappa | a + m$. Επομένως μπορούμε να γράψουμε την κλάση BAD συνολοθεωρητικά ως:

$$BAD := B_{q,\kappa,H} = \bigcup_{p|q} \bigcup_{m \in [1, 2H]} \{a < q^\kappa : p^\kappa | a + m\}.$$

Επίσης, ορίζουμε $B_{p,0} := \{a < q^\kappa : p^\kappa | a\}$, τότε για αυτήν ισχύουν τα εξής:

- (i) $|B_{p,0}| = q^\kappa / p^\kappa$.
- (ii) $|B_{p,0}| = |B_{p,m}|$, όπου $B_{p,m} := \{a < q^\kappa : p^\kappa | a + m\}$, για κάθε $m \in [1, 2H]$.

Εξ'ορισμού της B ισχύει ότι

$$|B| = \left| \bigcup_{p|q} \bigcup_{m \in [1, 2H]} \{a < q^\kappa : p^\kappa | a + m\} \right| = \left| \bigcup_{p|q} \bigcup_{m \in [1, 2H]} B_{p,m} \right|.$$

Έχουμε επομένως,

$$\begin{aligned} |B| &= \left| \bigcup_{p|q} \bigcup_{m \in [1, 2H]} B_{p,m} \right| = \left| \bigcup_{m \in [1, 2H]} \bigcup_{p|q} B_{p,m} \right| \leq 2H \sum_{p|q} |B_{p,m}| = \\ &= 2H \sum_{p|q} q^\kappa / p^\kappa < 2H 2^{-\kappa} q^\kappa \sum_{n \geq 2} \frac{1}{(n/2)^\kappa} < 2H 2^{-\kappa} q^\kappa \sum_{n \geq 2} \frac{1}{(n/2)^2} < 8H 2^{-\kappa} q^\kappa \sum_{n \geq 1} \frac{1}{n^2} = \\ &= \frac{8\pi^2}{6} H 2^{-\kappa} q^\kappa = O_H(2^{-\kappa} q^\kappa). \end{aligned}$$

Άρα τα στοιχεία της κλάσης BAD είναι αμελητέα και για αυτό θα ασχοληθούμε μόνο με τα στοιχεία που ανήκουν στην κλάση $GOOD$ και έτσι από εδώ και πέρα δεν θα ξαναγράψουμε ότι $a \in GOOD$.

Τώρα στην σχέση (6.9) μπορούμε να αντικαταστήσουμε κάτω από το τελευταίο άθροισμα το $(a + m_i, q^\kappa) = d_i$ με $d_i | a + m_i$.

Πράγματι, θα το δείξουμε για το d_1, m_1 και όμοια προκύπτει για τα d_2, m_2 .

Από την μία $(a + m_1, q^\kappa) | a + m_1$ και από την άλλη για τυχόν c με $c | a + m_1, c | d, c < d$, όπου $d = (a + m_1, q^\kappa)$, αν αναλύσουμε σε πρώτους παράγοντες έχουμε:

- $q = p_1^{\nu_1} \cdot \dots \cdot p_{n_1}^{\nu_{n_1}} \cdot A$, όπου $(A, p_1^{\nu_1} \cdot \dots \cdot p_{n_1}^{\nu_{n_1}}) = 1$.
- $a + m_1 = p_1^{l_1} \cdot \dots \cdot p_{n_1}^{l_{n_1}} \cdot B$, όπου $(B, p_1^{l_1} \cdot \dots \cdot p_{n_1}^{l_{n_1}}) = 1$.

και από την επιλογή των A και B έχουμε ότι $(A,B)=1$.

- $d = p_1^{m_1} \cdot \dots \cdot p_{n_1}^{m_{n_1}}$, με $m_i = \min\{l_i, \kappa_{\nu_i}\}$.

- $c = p_1^{l'_1} \cdot \dots \cdot p_{n_1}^{l'_{n_1}}$, με $l'_i \leq l_i$.

Ισχύει ότι $\left(\frac{a+m_1}{d}, q\right) = 1$, ισοδύναμα δηλαδή,

$$(p_1^{l_1-m_1} \cdot \dots \cdot p_{n_1}^{l_{n_1}-m_{n_1}} B, p_1^{\nu_1} \cdot \dots \cdot p_{n_1}^{\nu_{n_1}} A) = 1 \Leftrightarrow l_i - m_i = 0 \ \forall i \in \{1, \dots, n_1\} \Leftrightarrow l_i = m_i.$$

Έχουμε δηλαδή $d = p_1^{l_1} \cdot \dots \cdot p_{n_1}^{l_{n_1}}$. Εφόσον, $c|d$ και $c < d$, υπάρχει πρώτος p_i στην ανάλυση του c τέτοιο ώστε $l'_i < l_i$ και έτσι έχουμε $\left(\frac{a+m_1}{c}, q\right) \geq p_i > 1$ και εξ'ορισμού του χαρακτήρα *Dirichlet* ισχύει ότι $x\left(\frac{a+m_1}{c}\right) = 0$.

Άρα, ναι μεν το άθροισμα ως προς $d_i|a + m_i$ έχει περισσότερους προσθεταίους, αλλά από την άλλη οι περισσότεροι προσθεταίοι μας δίνουν ο καθένας τιμή μηδέν στον χαρακτήρα *Dirichlet*, επομένως δεν επηρεάζουν το άθροισμα.

Φτάνουμε έτσι στην σχέση:

$$\sum_{d_1, d_2 | q^\kappa} \tilde{x}(d_1) \overline{\tilde{x}(d_2)} \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{m_1, m_2 \in [1, H']} \sum_{a \in A'} x\left(\frac{a+m_1}{d_1}\right) \overline{x\left(\frac{a+m_2}{d_2}\right)} \leq K'' c_\varepsilon q^\kappa, \quad (6.10)$$

όπου $a \in A' \Leftrightarrow a \in [1, q^\kappa] : d_1|a + m_1, d_2|a + m_2$.

Τώρα εξετάζουμε την περίπτωση όπου $d_1, d_2 | q^\kappa$ και $d_1 \neq d_2$. Τότε προκύπτει ότι για τέτοια σταθεροποιημένα d_1, d_2 , αλλά και για σταθεροποιημένα $H' \in [H, 2H]$ και $m_1, m_2 \in [1, H']$ ισχύει ότι:

$$\sum_{a \in A'} x\left(\frac{a+m_1}{d_1}\right) \overline{x\left(\frac{a+m_2}{d_2}\right)} = 0,$$

όπου $a \in A' \Leftrightarrow a \in [1, q^\kappa] : d_1|a + m_1, d_2|a + m_2$.

Πράγματι, από το Θεώρημα 1.4.11 μπορούμε να εκφράσουμε τον χαρακτήρα x (τον οποίο όπως είπαμε πριν μπορούμε να θεωρήσουμε ότι είναι primitive) ως άθροισμα τριγωνομετρικών πολυωνύμων. Έστω ότι

$$x(n) = \frac{\tau_q(x)}{\sqrt{q}} \sum_{\xi \in (\mathbb{Z}/q\mathbb{Z})} \overline{x}(n) e^{-2\pi i \xi n / q}.$$

Άρα, η συνάρτηση συνάρτηση $f(n) = 1_{d_1|n} x(n/d_1)$ μπορεί να γραφεί ως

$$f(n) = 1_{d_1|n} \frac{\tau_q(x)}{\sqrt{q}} \sum_{(\xi, q)=1} \overline{x}(n) e^{-2\pi i \xi n / d_1 q}$$

και αν αναλύσουμε την $1_{d_1|n}$ ως τριγωνομετρικό πολυώνυμο η παραπάνω σχέση γράφεται ως

$$f(n) = c \sum_{(\xi, d_1 q)=1} K_\xi e^{-2\pi i \xi n / d_1 q}.$$

Επομένως για την συνάρτηση $F(a) = 1_{d_1|a+m_1} x\left(\frac{a+m_1}{d_1}\right)$, έχουμε

$$F(a) = c \sum_{(\xi, d_1 q)=1} K_\xi e^{-2\pi i \xi a / d_1 q},$$

όμοια για την συνάρτηση $G(a) = 1_{d_2|a+m_2} x\left(\frac{a+m_2}{d_2}\right)$, την γράφουμε

$$G(a) = c' \sum_{(\xi, d_2 q)=1} L_\xi e^{-2\pi i \xi a / d_2 q}.$$

Τώρα αν προσθέσουμε πάνω από όλα τα $a \in A'$

$$\begin{aligned} \sum_{a \in A'} x\left(\frac{a+m_1}{d_1}\right) \overline{x\left(\frac{a+m_2}{d_2}\right)} = \\ c'' \sum_{a \in A'} \left(\sum_{(\xi, d_1 q)=1} K_\xi e^{-2\pi i \xi a / d_1 q} \right) \overline{\left(\sum_{(\xi, d_2 q)=1} L_\xi e^{-2\pi i \xi a / d_2 q} \right)} = \\ c'' \sum_{(\xi_1, d_1 q)(\xi_2, d_2 q)=1} K_{\xi_1} \overline{L_{\xi_2}} \sum_{a \in A'} e^{-\frac{2\pi i}{q}(\xi_1/d_1 - \xi_2/d_2)a}. \end{aligned}$$

Έστω ότι υπάρχουν ξ_1, ξ_2 τέτοια ώστε $\frac{\xi_1}{d_1} = \frac{\xi_2}{d_2}$ τότε επειδή $(\xi_1, d_1 q) = 1$ και $(\xi_2, d_2 q) = 1$ από την ανάλυση σε πρώτους παράγοντες έχουμε

$$\xi_1 = p_1^{a'_1} \cdot \dots \cdot p_k^{a'_k} \cdot A, \xi_2 = p_1^{a''_1} \cdot \dots \cdot p_k^{a''_k} \cdot B,$$

με $(A, B)=1$ και για τον μέγιστο κοινό διαιρέτη $\underline{\xi}$ ισχύει $\underline{\xi} = p_1^{a''_1} \cdot \dots \cdot p_k^{a''_k}$, με $a''_i = \min\{a_i, a'_i\}$.

Όμοια, για τα d_1, d_2 έχουμε

$$d_1 = q_1^{b_1} \cdot \dots \cdot q_l^{b_l} \cdot C, d_2 = q_1^{b'_1} \cdot \dots \cdot q_l^{b'_l} \cdot D,$$

όπου $(C, D) = 1$ και για τον μέγιστο κοινό διαιρέτη $\underline{d}$ έχουμε $\underline{d} = q_1^{b''_1} \cdot \dots \cdot q_l^{b''_l}$, με $b''_i = \min\{b_i, b'_i\}$.

Από την υπόθεση $(\xi_1, d_1 q) = 1$ και $(\xi_2, d_2 q) = 1$ προκύπτει ότι $(A, C) = 1$ και $(B, D) = 1$. Τώρα, στην σχέση $\frac{\xi_1}{d_1} = \frac{\xi_2}{d_2}$, αν διαιρέσουμε με τους μέγιστους κοινούς διαιρέτες έχουμε:

$$\frac{\xi_1}{\underline{\xi}} \frac{d_2}{\underline{d}} = \frac{\xi_2}{\underline{\xi}} \frac{d_1}{\underline{d}}$$

και σύμφωνα με την προηγούμενη ανάλυση για να επιτευχθεί αυτή η ισότητα πρέπει $\xi_1 = \xi_2 = d_1 = d_2 = 1$, το οποίο είναι άτοπο αφού έχουμε ξεκινήσει με $d_1 \neq d_2$. Δηλαδή, εμφανίζονται διαφορετικές συχνότητες και τελικά το άθροισμα δίνει

$$\sum_{a \in A'} x\left(\frac{a+m_1}{d_1}\right) \overline{x\left(\frac{a+m_2}{d_2}\right)} = 0. \quad (6.11)$$

Άρα, ασχολούμαστε μόνο με $d_1 = d_2 = d$, επίσης $\tilde{x}(d)\overline{\tilde{x}(d)} = |\tilde{x}(d)| = 1$. Έτσι η σχέση (6.10) απλοποιείται περαιτέρω και γίνεται:

$$\sum_{d|q^\kappa-1} \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{m_1, m_2 \in [1, H']} \sum_{a \in A''} x\left(\frac{a+m_1}{d}\right) \overline{x\left(\frac{a+m_2}{d}\right)} \leq K'' c_\varepsilon q^\kappa, \quad (6.12)$$

όπου $a \in A'' \Leftrightarrow a \in [1, q^\kappa] : d|a+m_1, d|a+m_2$.

Έχουμε πλέον πραγματοποιήσει και την απαλοιφή του $\tilde{x}$ και έτσι μπορούμε να χειριστούμε καλύτερα τους χαρακτήρες Dirichlet χ .

Ξανά μαζεύουμε τα m_1, m_2 και στην θέση τους έχουμε πάλι m και έτσι φτάνουμε στην σχέση:

$$\sum_{d|q^\kappa-1} \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa]} \left| \sum_{m \in [1, H'] : d|a+m} x\left(\frac{a+m}{d}\right) \right|^2 \leq K'' c_\varepsilon q^\kappa.$$

Το άθροισμα πάνω από τα d είναι μη αρνητικό, έτσι μπορούμε να κάνουμε την απαλοιφή των d που δεν είναι της μορφής $d = q^i$ με $q^i < \sqrt{H}$ (εδώ, εφόσον η επιλογή του κ γίνεται μετά από αυτή του H , μπορούμε να διαλέξουμε αρκετά μεγάλο κ ώστε $\sqrt{H} < q^{\kappa-1}$) και να φτάσουμε σε μια σχέση στο αριστερό μέρος η οποία είναι μικρότερη από πριν και έτσι να πάρουμε την καινούρια ανίσωση:

$$\sum_{i: q^i < \sqrt{H}} \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa]} \left| \sum_{m \in [1, H'] : q^i|a+m} x\left(\frac{a+m}{q^i}\right) \right|^2 \leq K'' c_\varepsilon q^\kappa.$$

Στόχος μας πλέον είναι να εκμεταλλευτούμε τον μέσο όρο $\frac{1}{H} \sum_{H < H' \leq 2H}$ για να απλουστευτεί το άθροισμα ως προς το m .

Παρατηρούμε από την τριγωνική ανισότητα και την χρήση της ανισότητας *Cauchy – Schwarz* ότι για κάθε $H' \in (H, 3H/2]$ και για κάθε $a \in [1, q^\kappa]$ ισχύει ότι:

$$\begin{aligned} & \left| \sum_{H' < m \leq H' + q^i : q^i|a+m} x\left(\frac{a+m}{q^i}\right) \right|^2 = \\ & \left| \sum_{1 < m \leq H' + q^i : q^i|a+m} x\left(\frac{a+m}{q^i}\right) - \sum_{1 < m \leq H' : q^i|a+m} x\left(\frac{a+m}{q^i}\right) \right|^2 \leq \\ & \leq \left(\left| \sum_{1 < m \leq H' + q^i : q^i|a+m} x\left(\frac{a+m}{q^i}\right) \right| + \left| \sum_{1 < m \leq H' : q^i|a+m} x\left(\frac{a+m}{q^i}\right) \right| \right)^2 \leq \end{aligned}$$

$$\left(\left| \sum_{1 < m \leq H' + q^i: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 + \left| \sum_{1 < m \leq H': q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \right) (1^2 + 1^2) =$$

$$2 \left(\left| \sum_{1 < m \leq H' + q^i: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 + \left| \sum_{1 < m \leq H': q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \right).$$

Χρησιμοποιώντας αυτή την παρατήρηση έχουμε:

$$\sum_{i: q^i < \sqrt{H}} \frac{1}{H} \sum_{H < H' \leq 3H/2} \sum_{a \in [1, q^\kappa]} \left| \sum_{H' < m \leq H' + q^i: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \leq$$

$$2A_{i, H', a, m} + 2B_{i, H', a, m},$$

όπου για την ποσότητα $A_{i, H', a, m}$ έχουμε:

$$A_{i, H', a, m} = \sum_{i: q^i < \sqrt{H}} \frac{1}{H} \sum_{H < H' \leq 3H/2} \sum_{a \in [1, q^\kappa]} \left| \sum_{1 < m \leq H' + q^i: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \leq$$

$$\sum_{i: q^i < \sqrt{H}} \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa]} \left| \sum_{m \in [1, H']: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \leq K'' c_\varepsilon q^\kappa$$

(κανονικά για την ποσότητα $A_{i, H', a, m}$ είχαμε ότι $H < H' \leq 3H/2$ και $1 < m \leq H' + q^i$, άρα $1 \leq m \leq H' + \sqrt{H} \leq H' + H/2 \leq 3H/2 + H/2 = 2H$. Δηλαδή σε ένα άθροισμα από μη αρνητικούς αριθμούς βάλουμε περισσότερους προσθεταίους, χωρίς αυτοί ωστόσο να υπερβούν το $2H$).

και για την ποσότητα $B_{i, H', a, m}$ ισχύει:

$$B_{i, H', a, m} = \sum_{i: q^i < \sqrt{H}} \frac{1}{H} \sum_{H < H' \leq 3H/2} \sum_{a \in [1, q^\kappa]} \left| \sum_{1 < m \leq H': q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \leq$$

$$\sum_{i: q^i < \sqrt{H}} \frac{1}{H} \sum_{H < H' \leq 2H} \sum_{a \in [1, q^\kappa]} \left| \sum_{m \in [1, H']: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \leq K'' c_\varepsilon q^\kappa.$$

Έχουμε δηλαδή:

$$\sum_{i: q^i < \sqrt{H}} \frac{1}{H} \sum_{H < H' \leq 3H/2} \sum_{a \in [1, q^\kappa]} \left| \sum_{H' < m \leq H' + q^i: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \leq 4K'' c_\varepsilon q^\kappa.$$

Στην συνέχεια εφόσον για τον μέσο όρο

$$\frac{1}{H} \sum_{H' < H' \leq 3H/2} \sum_{i: q^i < \sqrt{H}} \sum_{a \in [1, q^\kappa]} \left| \sum_{H' < m \leq H' + q^i: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2,$$

ισχύει ότι δεν ξεπερνάει την ποσότητα $4K''c_\varepsilon q^\kappa$, χρησιμοποιώντας την αρχή του περιστεριώνα έχουμε ότι υπάρχει $H'(\omega) \in (H, 3H/2]$ (το οποίο είναι στοχαστικό, αφού για διαφορετική επιλογή του ω αλλάζει το $q(\omega)$ άρα και η επιλογή του H' και αντί για $H'(\omega)$ θα γράφουμε απλά H') τέτοιο ώστε:

$$\sum_{i: q^i < \sqrt{H}} \sum_{a \in [1, q^\kappa]} \left| \sum_{H' < m \leq H' + q^i: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \leq 4K''c_\varepsilon q^\kappa.$$

Στην συνέχεια δουλεύουμε σε δύο βήματα για να απλοποιήσουμε την παραπάνω σχέση:

Βήμα 1

Με αλλαγή μεταβλητής έχουμε: $m' = m - H'$, άρα $m = m' + H'$. Έτσι,

$$H' < m \leq H' + q^i \Leftrightarrow H' < m' + H' \leq H' + q^i \Leftrightarrow 0 < m' \leq q^i.$$

Φτάνουμε δηλαδή στην σχέση:

$$\sum_{i: q^i < \sqrt{H}} \sum_{a \in [1, q^\kappa]} \left| \sum_{0 < m' \leq q^i: q^i | a+m'+H'} x \left(\frac{a+m'+H'}{q^i} \right) \right|^2 \leq 4K''c_\varepsilon q^\kappa.$$

Κάνοντας εκ νέου αλλαγή μεταβλητής: $a' = a + H'$, άρα $a = a' - H'$. Επειδή, οι όροι που εμφανίζονται είναι μη-αρνητικοί, με απαλοιφή όρων, έχουμε:

$$1 \leq a \leq q^\kappa \Rightarrow 1 < a \leq q^\kappa/2 \Leftrightarrow 1 < a' - H' \leq q^\kappa/2.$$

Τώρα, επιλέγοντας αρκετά μεγάλο κ έτσι ώστε $q^\kappa/2 + H' < q^\kappa$ έχουμε:

$$1 < a' - H' \leq q^\kappa/2 \Leftrightarrow H' < a' \leq q^\kappa/2 + H'$$

και τελικά με απαλοιφή κάποιων όρων ακόμα:

$$H' < a' \leq q^\kappa/2 + H' \Rightarrow H' < a' \leq q^\kappa/2.$$

Φτάνουμε επομένως στην σχέση:

$$\sum_{i:q^i < \sqrt{H}} \sum_{a' \in (H', q^\kappa/2]} \left| \sum_{0 < m' \leq q^i: q^i | a' + m'} x \left(\frac{a' + m'}{q^i} \right) \right|^2 \leq 4K'' c_\varepsilon q^\kappa \Leftrightarrow$$

$$\sum_{i:q^i < \sqrt{H}} \sum_{a \in (H', q^\kappa/2]} \left| \sum_{0 < m \leq q^i: q^i | a + m} x \left(\frac{a + m}{q^i} \right) \right|^2 \leq 4K'' c_\varepsilon q^\kappa.$$

Βήμα 2

Τώρα για τα a τα οποία ανήκουν στο διάστημα $[1, H']$ έχουμε:

Αρχικά, για φιξαρισμένο $a \in [1, H']$ θέλουμε να δούμε τι μπορεί να μας δώσει η ποσότητα $\left| \sum_{0 < m \leq q^i: q^i | a + m} x \left(\frac{a + m}{q^i} \right) \right|^2$. Εφόσον $0 < m \leq q^i$, ισχύει ότι:

(1) Αν $q^i | a$, τότε μόνο για $m = q^i$ ισχύει ότι $q^i | a + m$. Άρα το πολύ 2 διαιρέτες, δηλαδή το πολύ 2 προσθετέοι.

(2) Αν $q^i \nmid a$, τότε $a \equiv \kappa \pmod{q^i}$, με $0 < \kappa < q^i$. Άρα, μόνο για $m = q^i - \kappa \Rightarrow q^i | a + m$. Δηλαδή, το πολύ 1 διαιρέτης, άρα 1 προσθετέος σε αυτή την περίπτωση.

Από (1) και (2) έχουμε ότι:

$$\left| \sum_{0 < m \leq q^i: q^i | a + m} x \left(\frac{a + m}{q^i} \right) \right|^2 \leq (1 + 1)^2 = 4$$

Χρησιμοποιώντας αυτή την παρατήρηση, φτάνουμε στο συμπέρασμα:

$$\sum_{i:q^i < \sqrt{H}} \sum_{a \in [1, H']} \left| \sum_{0 < m \leq q^i: q^i | a + m} x \left(\frac{a + m}{q^i} \right) \right|^2 \leq 4H' \frac{1}{2} \log H$$

$$< 4 \frac{3H}{2} \frac{1}{2} \log H = 3H \log H < 3q^\kappa,$$

αρκεί η επιλογή του κ να είναι αρκετά μεγάλη ώστε η ποσότητα q^κ να απορροφήσει την $H \log H$.

Με τα παραπάνω βήματα έχουμε ότι:

$$\sum_{i:q^i < \sqrt{H}} \sum_{a \in [1, q^\kappa/2]} \left| \sum_{0 < m \leq q^i: q^i | a+m} x \left(\frac{a+m}{q^i} \right) \right|^2 \leq 4K''c_\varepsilon q^\kappa + 3q^\kappa = (4K''c_\varepsilon + 3)q^\kappa.$$

Παρατηρούμε ότι για φιζαρισμένο a υπάρχει ακριβώς ένα m στο άθροισμα τέτοιο ώστε

$$\frac{a+m}{q^i} = \left\lfloor \frac{a}{q^i} \right\rfloor + 1.$$

Πράγματι, διακρίνουμε περιπτώσεις:

- Αν $\frac{a}{q^i} \in \mathbb{Z}$, τότε επειδή $q^i | a+m$ και $0 < m \leq q^i \Rightarrow m = q^i$ και έτσι έχουμε $\frac{a+m}{q^i} = \left\lfloor \frac{a}{q^i} \right\rfloor + 1$.
- Αν $\frac{a}{q^i} \notin \mathbb{Z}$, τότε $a \equiv \kappa \pmod{q^i}$, άρα $\kappa < q^i$ και $0 < m < q^i$, άρα $m \equiv m \pmod{q^i}$ και $q^i | a+m \Rightarrow \kappa + m \equiv 0 \pmod{q^i}$, δηλαδή $q^i | k+m = q^i$.

Έχουμε από την μία:

$$\left\lfloor \frac{a}{q^i} \right\rfloor + 1 = \left\lfloor \frac{lq^i + k}{q^i} \right\rfloor + 1 = \frac{lq^i}{q^i} + 1 = l + 1$$

και από την άλλη

$$\frac{a+m}{q^i} = \frac{lq^i + \kappa + m}{q^i} = l + \frac{q^i}{q^i} = l + 1.$$

Άρα, έχουμε $\frac{a+m}{q^i} = \left\lfloor \frac{a}{q^i} \right\rfloor + 1$.

Επομένως το άθροισμα γίνεται:

$$\sum_{i:q^i < \sqrt{H}} \sum_{a \in [1, q^\kappa/2]} \left| x \left(\left\lfloor \frac{a}{q^i} \right\rfloor + 1 \right) \right|^2 \leq (4K''c_\varepsilon + 3)q^\kappa.$$

Θα απλοποιήσουμε το παραπάνω άθροισμα με μια αλλαγή μεταβλητής και απαλοιφή κάποιων όρων ακόμα.

Θέτουμε $b := \left\lfloor \frac{a}{q^i} \right\rfloor + 1$, τότε:

$$1 \leq a \leq \frac{q^\kappa}{2} \Rightarrow \left\lfloor \frac{1}{q^i} \right\rfloor \leq \left\lfloor \frac{a}{q^i} \right\rfloor \leq \left\lfloor \frac{q^{\kappa-i}}{2} \right\rfloor \Rightarrow$$

$$0 + 1 \leq \left\lfloor \frac{a}{q^i} \right\rfloor + 1 \leq \left\lfloor \frac{q^{\kappa-i}}{2} \right\rfloor + 1 \Rightarrow 1 \leq b \leq \left\lfloor \frac{q^{\kappa-i}}{2} \right\rfloor \Rightarrow 1 \leq b \leq \left\lfloor \frac{q^{\kappa-i}}{4} \right\rfloor,$$

όπου στις τελευταίες δύο συνεπαγωγές γίνανε απαλοιφές όρων. Τέλος παρατηρούμε ότι:

- Για κάθε $a \in [1, q^i)$ ισχύει ότι $\left\lfloor \frac{a}{q^i} \right\rfloor = 0$, άρα αν αθροίσουμε πάνω από όλα αυτά τα a θα πάρουμε $q^i - 1$ φορές τον προσθεταίο $x(0 + 1)$.
- Για κάθε $a \in [q^i, 2q^i)$ ισχύει ότι $\left\lfloor \frac{a}{q^i} \right\rfloor = 1$, άρα αν αθροίσουμε πάνω από όλα αυτά τα a θα πάρουμε q^i φορές τον προσθετέο $x(1 + 1)$.
- Επαγωγικά βλέπουμε ότι:

$$\sum_{i: q^i < \sqrt{H}} q^i \sum_{b \in [1, \frac{q^{\kappa-i}}{4}]} |x(b)|^2 \leq (4K''c_\varepsilon + 3)q^\kappa.$$

Τώρα, η συνάρτηση $b \mapsto |x(b)|^2$ είναι q περιοδική και για την μέση τιμή της ισχύει :

$$\frac{|x(1)|^2 + \dots + |x(q)|^2}{q} = \frac{\phi(q)}{q} > \frac{1}{q} > 1 \cdot O_\varepsilon^{-1}(1) = C_\varepsilon^{-1}.$$

Με βάση την ανίσωση για την μέση τιμή θέλουμε να δείξουμε ότι:

$$\sum_{b \in [1, \frac{q^{\kappa-i}}{4}]} |x(b)|^2 \geq \frac{C_\varepsilon^{-1}}{8} q^{\kappa-i}.$$

Πράγματι, θεωρούμε τις ποσότητες: $A = \left\lfloor \left\lfloor \frac{q^{\kappa-i}}{4} \right\rfloor / q \right\rfloor$, $|B| = \left\lfloor \frac{q^{\kappa-i}}{4} \right\rfloor - |A|$

(επομένως, $|B| \leq q$) και $|\Gamma| = \left\lfloor \left[1, \left\lfloor \frac{q^{\kappa-i}}{4} \right\rfloor \right] \right\rfloor$. Ισχύει ότι μπορούμε να έχουμε, για μεγάλο κ , $\frac{|A|}{|\Gamma|} \geq \frac{3}{4}$. Επίσης για αρκετά μεγάλο κ έχουμε $\frac{q}{|\Gamma|} = \frac{q}{\left\lfloor \frac{q^{\kappa-i}}{4} \right\rfloor} < \frac{1}{C_\varepsilon} \frac{1}{4}$. Τότε,

$$\sum_{b \in [1, \frac{q^{\kappa-i}}{4}]} \frac{|x(b)|^2}{\left\lfloor \frac{q^{\kappa-i}}{4} \right\rfloor} = \frac{|A|}{|\Gamma|} \sum_{b \in A} \frac{|x(b)|^2}{\left\lfloor \frac{q^{\kappa-i}}{4} \right\rfloor} + \frac{|B|}{|\Gamma|} \sum_{b \in B} \frac{|x(b)|^2}{\left\lfloor \frac{q^{\kappa-i}}{4} \right\rfloor} \geq$$

$$\geq \frac{|A|}{|\Gamma|} C_\varepsilon^{-1} - \frac{q}{|\Gamma|} 1 \geq \frac{3}{4} C_\varepsilon^{-1} - \frac{1}{4} C_\varepsilon^{-1} = \frac{C_\varepsilon^{-1}}{2} \Leftrightarrow$$

$$\sum_{b \in \left[1, \frac{q^{\kappa-i}}{4}\right]} \frac{|x(b)|^2}{\left[\frac{q^{\kappa-i}}{4}\right]} \geq \frac{C_\varepsilon^{-1}}{2} \Leftrightarrow \sum_{b \in \left[1, \frac{q^{\kappa-i}}{4}\right]} |x(b)|^2 > \frac{C_\varepsilon^{-1}}{8} q^{\kappa-i}$$

και έτσι το ζητούμενο έχει δειχθεί.

Τέλος, γυρίζοντας στην σχέση:

$$\sum_{i: q^i < \sqrt{H}} q^i \sum_{b \in \left[1, \frac{q^{\kappa-i}}{4}\right]} |x(b)|^2 \leq (4K''c_\varepsilon + 3)q^\kappa$$

και χρησιμοποιώντας την τελευταία ανίσωση έχουμε:

$$(4K''c_\varepsilon + 3)q^\kappa \geq \sum_{i: q^i < \sqrt{H}} q^i \sum_{b \in \left[1, \frac{q^{\kappa-i}}{4}\right]} |x(b)|^2 \geq \sum_{i: q^i < \sqrt{H}} q^i \frac{C_\varepsilon^{-1}}{8} q^{\kappa-i}$$

$$= \frac{C_\varepsilon^{-1}}{8} \sum_{i: q^i < \sqrt{H}} q^\kappa = \frac{C_\varepsilon^{-1}}{8} q^\kappa \sum_{i: q^i < \sqrt{H}} 1 = \frac{C_\varepsilon^{-1}}{8} q^\kappa \frac{1}{2} \log H.$$

Δηλαδή, έχουμε ότι:

$$\log H < 4(4K''c_\varepsilon + 3)C_\varepsilon,$$

το οποίο καταλήγει σε άτοπο αφού η επιλογή του H έπεται σε σχέση με αυτή του ε και έτσι για αρκούντως μεγάλο H , το αριστερό μέλος της ανίσωσης είναι μεγαλύτεροι από το δεξί. $\square$

7 Βιβλιογραφία

[1] T. M. Apostol, Introduction to analytic number theory. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] Convergence of Probability Measures, second edition Patrick Billingsley Copyright 1999 by John Wiley & Sons, Inc

[3] G. B. Folland: Real Analysis — Modern Techniques and their Applications, second edition Copyright 1999 John Wiley & Sons.

[4] Introduction to Analytic Number Theory Math 531 Lecture Notes, Fall 2005 A.J. Hildebrand Department of Mathematics University of Illinois <http://www.math.uiuc.edu/hildebr/ant> Version 2013.01.07

[5] T. Tao, The Erdos discrepancy problem. arXiv:1509.05363

[6] T. Tao, The logarithmically averaged Chowla and Elliott conjectures for two-point correlations, preprint. arXiv:1509.05422

[7] H. Montgomery, Ten lectures on the interface between analytic number theory and harmonic analysis, volume 84 of CBMS Regional Conference Series in Mathematics. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994

[8] A. Granville, K. Soundararajan, Large character sums: pretentious characters and the Pólya-Vinogradov theorem, J. Amer. Math. Soc. 20 (2007), no. 2, 357–384.

[9] K. Matomäki, M. Radziwiłł, A note on the Liouville function in short intervals, preprint. arXiv:1502.02374.