ΚΕΦΑΛΑΙΟ 1

Ο ασυμπτωτικός τύπος των Hardy-Littlewood

1.1 Η μέθοδος του κύκλου

Έστω k και s φυσικοί αριθμοί. Συμβολίζουμε με $r_{k,s}(N)$ το πλήθος των αναπαραστάσεων του N ως αθροίσματος s θετικών k-οστών δυνάμεων, δηλαδή το πλήθος των s-άδων $(x_1,\dots,x_s)$ φυσικών αριθμών με

$$N = x_1^k + \cdots + x_s^k.$$

Το πρόβλημα του Waring είναι το ερώτημα αν κάθε μη αρνητικός ακέραιος είναι το άθροισμα φραγμένου πλήθους k-οστών δυνάμεων. Αφού ο $1 = 1^k$ είναι k-οστή δύναμη, το πρόβλημα είναι ισοδύναμο με το να δείξουμε ότι

$$r_{k,s}(N) > 0$$

για κάποιον s και για όλους τους αρκετά μεγάλους φυσικούς N. Ο Hilbert έδωσε πρώτος θετική απάντηση στο πρόβλημα του Waring το 1909. Δέκα χρόνια αργότερα, οι Hardy και Littlewood κατόρθωσαν να βρουν έναν πολύ όμορφο ασυμπτωτικό τύπο για τον $r_{k,s}(N)$. Απέδειξαν ότι, για $s \geqslant s_0(k)$, υπάρχει $\delta = \delta(s,k) > 0$ τέτοιος ώστε

$$r_{k,s}(N) = \mathcal{G}(N)\Gamma\Big(1+\frac{1}{k}\Big)^s\Gamma\Big(\frac{s}{k}\Big)^{-1}N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\delta}), \tag{1.1.1}$$

όπου $\Gamma(x)$ είναι η συνάρτηση Γάμμα και $\mathcal{G}(N)$ είναι η λεγόμενη «ιδιάζουσα σειρά», μια αριθμητική συνάρτηση που είναι ομοιόμορφα φραγμένη, από πάνω και από κάτω, από θετικές σταθερές που εξαρτώνται μόνο από τους k και s. Θα αποδείξουμε ότι ο ασυμπτωτικός τύπος (1.1.1) ισχύει για τον $s_0(k) = 2^k + 1$.

Οι Hardy και Littlewood χρησιμοποίησαν τη «μέθοδο του κύκλου» για να αποδείξουν αυτό το θεώρημα. Η βασική ιδέα της μεθόδου του κύκλου είναι απλή. Έστω A τυχόν σύνολο μη αρνητικών ακεραίων. Η γεννήτρια συνάρτηση για το A είναι η

$$f(z) = \sum_{a\in A} z^a.$$

Μπορούμε να θεωρήσουμε την $f(z)$ είτε ως τυπική δυναμοσειρά ως προς z είτε ως τη σειρά Taylor μιας αναλυτικής συνάρτησης που συγκλίνει στον ανοικτό μοναδιαίο δίσκο $|z| < 1$. Τόσο στην πρώτη όσο και στην δεύτερη περίπτωση, έχουμε

$$f(z)^s = \sum_{N=0}^{\infty} r_{A,s}(N) z^N,$$

όπου $r_{A,s}(N)$ είναι το πλήθος των αναπαραστάσεων του N ως αθροίσματος s στοιχείων του A, δηλαδή, το πλήθος των λύσεων της εξίσωσης

$$N = a_1 + a_2 + \cdots + a_s$$

με

$$a_1, a_2, \ldots, a_s \in A.$$

Από το θεώρημα του Cauchy, μπορούμε να δώσουμε μια έκφραση για τον $r_{k,s}(N)$ ολοκληρώνοντας: έχουμε

$$r_{A,s}(N) = \frac{1}{2\pi i} \int_{|z|=\varrho} \frac{f(z)^s}{z^{N+1}}\, dz$$

για κάθε $\varrho \in (0,1)$.

Αυτή είναι η αρχική μορφή της «μεθόδου του κύκλου», η οποία εισήχθη από τους Hardy, Littlewood και Ramanujan το 1918–20. Υπολόγισαν αυτό το ολοκλήρωμα χωρίζοντας τον κύκλο πάνω στον οποίο γίνεται η ολοκλήρωση σε δύο ξένα σύνολα, τα «μείζονα τόξα» και τα «ελλάσσονα τόξα». Στις κλασικές εφαρμογές για το πρόβλημα του Waring, το ολοκλήρωμα πάνω από τα ελλάσσονα τόξα είναι αμελητέο, και τοολοκλήρωμα πάνω από τα μείζονα τόξα δίνει τον βασικό όρο στην εκτίμηση για τον $r_{A,s}(N)$.

Ο Vinogradov απλούστευσε και βελτίωσε σε μεγάλο βαθμό τη μέθοδο του κύκλου. Παρατήρησε ότι για τη μελέτη του $r_{A,s}(N)$, μπορούμε να αντικαταστήσουμε τη δυναμοσειρά $f(z)$ με το πολυώνυμο

$$p(z) = \sum_{\substack{a \in A \\ a \leqslant N}} z^a.$$

Τότε,

$$p(z)^s = \sum_{m=0}^{sN} r_{A,s}^{(N)}(m) z^m,$$

όπου $r_{A,s}^{(N)}(m)$ είναι το πλήθος των αναπαραστάσεων του m ως αθροίσματος s στοιχείων του A που δεν ξεπερνούν τον N. Ειδικότερα, αφού τα στοιχεία του A είναι μη αρνητικά, έχουμε $r_{A,s}^{(N)}(m) = r_{A,s}(m)$ για $m \leqslant N$ και $r_{A,s}^{(N)}(m) = 0$ για $m > sN$. Αν θέσουμε

$$z = e(\alpha) = e^{2\pi i \alpha},$$

τότε παίρνουμε το τριγωνομετρικό πολυώνυμο

$$F(\alpha) = p(e(\alpha)) = \sum_{\substack{a \in A \\ a \leqslant N}} e(a\alpha)$$

και

$$F(\alpha)^s = \sum_{m=0}^{sN} r_{A,s}^{(N)}(m) e(m\alpha).$$

Χρησιμοποιώντας το γεγονός ότι οι συναρτήσεις $e(n\alpha)$ σχηματίζουν ορθοκανονικό σύστημα, παίρνουμε

$$r_{A,s}(N) = \int_0^1 F(\alpha)^s e(-N\alpha)\, d\alpha.$$

Στις εφαρμογές, το δύσκολο μέρος του επιχειρήματος είναι φυσικά το να δοθούν εκτιμήσεις για το ολοκλήρωμα.

Για να εφαρμόσουμε τη μέθοδο του κύκλου στο πρόβλημα του κύκλου, θεωρούμε $k \geqslant 2$ και το σύνολο A των k-οστών δυνάμεων. Έστω $r_{k,s}(N)$ το πλήθος των αναπαραστάσεων του N ως αθροίσματος s θετικών k-οστών δυνάμεων. Θέτουμε

$$P = \lfloor N^{1/k} \rfloor.$$

Τότε,

$$F(\alpha) = \sum_{\substack{a \in A \\ a \leqslant N}} e(a\alpha) = \sum_{n=1}^{P} e(\alpha n^k)$$

και

$$r_{k,s}(N) = \int_0^1 F(\alpha)^s e(-\alpha N)\, d\alpha.$$

1.2 Το πρόβλημα του Waring για $k = 1$

Στην περίπτωση $k = 1$, το θεώρημα που ακολουθεί δίνει ακριβή τύπο για τον $r_{1,s}(N)$.

Θεώρημα 1.2.1. *Έστω $s \geqslant 1$. Τότε,*

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

για κάθε $N \in \mathbb{N}$.

Απόδειξη. Έστω $N \geqslant s$. Παρατηρούμε ότι έχουμε αναπαράσταση

$$N = a_1 + \cdots + a_s$$

του N ως αθροίσματος s φυσικών αριθμών αν και μόνο αν έχουμε αναπαράσταση

$$N - s = (a_1 - 1) + \cdots + (a_s - 1)$$

του $N - s$ ως αθροίσματος s μη αρνητικών ακεραίων. Συνεπώς,

$$r_{1,s}(N) = R_{1,s}(N - s),$$

όπου $R_{1,s}(N)$ είναι το πλήθος των αναπαραστάσεων του N ως αθροίσματος s μη αρνητικών ακεραίων.

Θα δώσουμε δύο αποδείξεις του θεωρήματος. Η πρώτη είναι συνδυαστική. Αρχικά υπολογίζουμε τον $R_{1,s}(N)$ για κάθε μη αρνητικό ακέραιο N. Έστω $N = a_1 + \cdots + a_s$ μια διαμέριση σε μη αρνητικούς ακεραίους. Είναι σαν να έχουμε $N + s - 1$ κουτιά, να χρωματίζουμε τα πρώτα a_1 κόκκινα, το επόμενο γαλάζιο, τα επόμενα a_2 κόκκινα, το επόμενο γαλάζιο, και ούτω καθεξής. Θα υπάρχουν ακριβώς $s-1$ γαλάζια κουτιά. Αντίστροφα, αν επιλέξουμε $s-1$ από τα $N+s-1$ κουτιά και τα χρωματίσουμε γαλάζια, και αν χρωματίσουμε τα υπόλοιπα κουτιά κόκκινα, παίρνουμε μια διαμέριση του N σε s μη αρνητικά μέρη ως εξής. Ορίζουμε a_1 το πλήθος των κόκκινων κουτιών πριν από το πρώτο γαλάζιο, a_2 το πλήθος των κόκκινων κουτιών ανάμεσα στο πρώτο και το δεύτερο γαλάζιο κουτί, και γενικά, για $j = 2, \ldots, s-1$ ορίζουμε a_j το πλήθος των κόκκινων κουτιών ανάμεσα στο $(j-1)$-οστό και το j-οστό γαλάζιο κουτί. Τέλος, ορίζουμε a_s να είναι το πλήθος των κόκκινων κουτιών που βρίσκονται μετά από το τελευταίο γαλάζιο. Με αυτόν τον τρόπο έχουμε μια 1-1 αντιστοιχία ανάμεσα στα υποσύνολα του $\{1, \ldots, N+s-1\}$ που έχουν $s-1$ στοιχεία (τις επιλογές των κουτιών που χρωματίζουμε γαλάζια) και τις αναπαραστάσεις του N ως αθροίσματος s μη αρνητικών ακεραίων. Έπεται ότι το πλήθος αυτών των αναπαραστάσεων ισούται με $\binom{N+s-1}{s-1}$, άρα

$$r_{1,s}(N) = R_{1,s}(N-s) = \binom{N-1}{s-1}.$$

Αυτή είναι η πρώτη απόδειξη του θεωρήματος.

Υπάρχει επίσης μια απλή αναλυτική απόδειξη. Η σειρά

$$f(z) = \sum_{N=0}^{\infty} z^N = \frac{1}{1-z}$$

συγκλίνει αν $|z| < 1$, και

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

Επίσης έχουμε

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

Συνεπώς,

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

όπως ισχυρίζεται το θεώρημα. □

1.3 Η διάσπαση Hardy-Littlewood

Όταν $k \geqslant 2$, δεν είναι εύκολο να υπολογίσουμε - ή ακόμα και να εκτιμήσουμε - τον $r_{k,s}(N)$ για μεγάλα N. Οι Hardy και Littlewood κατόρθωσαν να αποδείξουν έναν ασυμπτωτικό τύπο για τον $r_{k,s}(N)$ για κάθε $k \geqslant 2$ και $s \geqslant s_0(k)$. Σε αυτό το κεφάλαιο αποδεικνύουμε τον ασυμπτωτικό τύπο των Hardy-Littlewood για $s \geqslant 2^k + 1$. Για $N \geqslant 2^k$ θέτουμε

$$P = \lfloor N^{1/k} \rfloor \tag{1.3.1}$$

και

$$F(\alpha) = \sum_{m=1}^{P} e(\alpha m^k). \tag{1.3.2}$$

Το τριγωνομετρικό πολυώνυμο $F(\alpha)$ είναι η γεννήτρια συνάρτηση για την αναπαράσταση του N ως αθροίσματος k-οστών δυνάμεων. Η βάση για τη μέθοδο του κύκλου είναι ο απλός τύπος

$$r_{k,s}(N) = \int_0^1 F(\alpha)^s e(-N\alpha)\, d\alpha. \tag{1.3.3}$$

Δεν μπορούμε να υπολογίσουμε αυτό το ολοκλήρωμα ακριβώς μέσω στοιχειωδών συναρτήσεων. Εξετάζοντας το όμως προσεκτικά, θα αποδείξουμε τον ασυμπτωτικό τύπο των Hardy-Littlewood.

Το πρώτο βήμα είναι να χωρίσουμε το μοναδιαίο διάστημα $[0, 1]$ σε δύο ξένα σύνολα, τα *μείζονα τόξα* $\mathcal{M}$ και τα *ελλάσσονα τόξα* $\Updownarrow$, και να εκτιμήσουμε το ολοκλήρωμα χωριστά πάνω από αυτά τα δύο σύνολα. Τα μείζονα τόξα αποτελούνται από όλους τους πραγματικούς αριθμούς $\alpha \in [0, 1]$ οι οποίοι προσεγγίζονται, με μία έννοια, καλά από ρητούς αριθμούς, και τα ελλάσσονα τόξα αποτελούνται από τους αριθμούς $\alpha \in [0, 1]$ που δεν προσεγγίζονται καλά από ρητούς. Παρόλο που το μεγαλύτερο μέρος του μοναδιαίου διαστήματος περιέχεται στα ελλάσσονα τόξα, από την ανισότητα του Weyl και το λήμμα του Hua μπορούμε να συμπεράνουμε ότι το ολοκλήρωμα της $F(\alpha)^s e(-N\alpha)$ στα ελλάσσονα τόξα είναι αμελητέο. Το ολοκλήρωμα στα μείζονα τόξα παραγοντοποιείται στο γινόμενο δύο όρων: του «ιδιάζοντος ολοκληρώματος» $J(N)$ και της «ιδιάζουσας σειράς» $\mathcal{G}(N)$. Το ιδιάζον ολοκλήρωμα υπολογίζεται μέσω της συνάρτησης Γάμμα, και για την ιδιάζουσα σειρά δίνουμε εκτιμήσεις χρησιμοποιώντας στοιχειώδη θεωρία αριθμών.

Τα μείζονα και ελλάσσονα τόξα κατασκευάζονται ως εξής. Έστω $N \geqslant 2^k$. Τότε, $\lfloor N^{1/k} \rfloor \geqslant 2$. Επιλέγουμε

$$0 < \nu < 1/5.$$

Για

$$1 \leqslant q \leqslant P^\nu, \quad 0 \leqslant a \leqslant q, \quad (a, q) = 1,$$

θέτουμε

$$\mathcal{M}(q, a) = \Big\{\alpha \in [0, 1] : \Big|\alpha - \frac{a}{q}\Big| \leqslant \frac{1}{P^{k-\nu}}\Big\}$$

και

$$\mathcal{M} = \bigcup_{1 \leqslant q \leqslant P^\nu} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \mathcal{M}(q, a).$$

Το διάστημα $\mathcal{M}(q,a)$ λέγεται *μείζον τόξο*, και το $\mathcal{M}$ είναι το σύνολο όλων των μειζόνων τόξων. Βλέπουμε ότι

$$\mathcal{M}(1,0) = \Big[0, \frac{1}{P^{k-\nu}}\Big],$$
$$\mathcal{M}(1,1) = \Big[1 - \frac{1}{P^{k-\nu}}, 1\Big],$$

και

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

για $q \geqslant 2$. Τα μείζονα τόξα αποτελούνται από όλους τους πραγματικούς αριθμούς $\alpha \in [0,1]$ που προσεγγίζονται καλά από ρητούς με την έννοια ότι είναι κοντά, σε απόσταση $P^{\nu-k}$, από κάποιον ρητό αριθμό με παρονομαστή το πολύ ίσο με P^{ν}.

Αν $\alpha \in \mathcal{M}(q,a) \cap \mathcal{M}(q',a')$ και $a/q \neq a'/q'$, τότε $|aq' - a'q| \geqslant 1$ και

$$\begin{aligned}\frac{1}{P^{2\nu}} &\leqslant \frac{1}{qq'}\\ &\leqslant \frac{|aq' - a'q|}{qq'}\\ &= \Big|\frac{a}{q} - \frac{a'}{q'}\Big|\\ &\leqslant \Big|\alpha - \frac{a}{q}\Big| + \Big|\alpha - \frac{a'}{q'}\Big|\\ &\leqslant \frac{2}{P^{k-\nu}},\end{aligned}$$

και έτσι προκύπτει $P^{k-3\nu} \leqslant 2$ το οποίο δεν μπορεί να ισχύει για $P \geqslant 2$ και $k \geqslant 2$. Συνεπώς, τα μείζονα τόξα $\mathcal{M}(q,a)$ είναι ξένα ανά δύο.

Το μέτρο του συνόλου $\mathcal{M}(1,0) \cup \mathcal{M}(1,1)$ είναι $2P^{\nu-k}$, και, για κάθε $q \geqslant 2$ με $(a,q) = 1$, το μέτρο του μείζονος τόξου $\mathcal{M}(q,a)$ είναι $2P^{\nu-k}$. Για κάθε $q \geqslant 2$ υπάρχουν ακριβώς $\varphi(q)$ θετικοί ακέραιοι a τέτοιοι ώστε $1 \leqslant a \leqslant q$ και $(q,a) = 1$. Έπεται ότι το μέτρο του συνόλου $\mathcal{M}$ των μειζόνων τόξων είναι

$$\mu(\mathcal{M}) = \frac{2}{P^{k-\nu}} \sum_{1 \leqslant q \leqslant P^{\nu}} \varphi(q) \leqslant \frac{2}{P^{k-\nu}} \sum_{1 \leqslant q \leqslant P^{\nu}} q \leqslant \frac{2}{P^{k-\nu}} \frac{P^{\nu}(P^{\nu}+1)}{2} \leqslant \frac{2}{P^{k-3\nu}}, \tag{1.3.4}$$

που τείνει στο 0 όταν το P τείνει στο άπειρο.

Το σύνολο

$$\Updownarrow = [0,1] \setminus \mathcal{M}$$

είναι το σύνολο των *ελλασσόνων τόξων*. Αυτό το σύνολο είναι πεπερασμένη ένωση ανοικτών διαστημάτων και αποτελείται από όλους τους $\alpha \in [0,1]$ που δεν προσεγγίζονται καλά από ρητούς. Το μέτρο του συνόλου των ελλασσόνων τόξων είναι

$$\mu(\Updownarrow) = 1 - \mu(\mathcal{M}) > 1 - \frac{2}{P^{k-3\nu}}.$$

Αν και το μέτρο του συνόλου $\Updownarrow$ είναι μεγάλο με την έννοια ότι τείνει στο 1 όταν το P τείνει στο άπειρο, στην επόμενη παράγραφο θα δείξουμε ότι το ολοκλήρωμα πάνω από τα ελλάσσονα τόξα συνεισφέρει μόνο αμελητέο ποσοστό στο $r_{k,s}(N)$.

1.4 Τα ελάσσονα τόξα

Αποδεικνύουμε εδώ ότι το ολοκλήρωμα πάνω από τα ελλάσσονα τόξα είναι μικρό.

Θεώρημα 1.4.1. *Έστω $k \geqslant 2$ και $s \geqslant 2^k + 1$. Υπάρχει $\delta_1 > 0$ τέτοιος ώστε*

$$\int_{\mathcal{M}} F(\alpha)^s e(-N\alpha)\, d\alpha = O(P^{s-k-\delta_1}),$$

με την σταθερά (στο O) να εξαρτάται μόνο από τους k και s.

Απόδειξη. Εφαρμόζοντας το Θεώρημα **;;** (θεώρημα του Dirichlet) με $Q = P^{k-\nu}$, για κάθε πραγματικό αριθμό α μπορούμε να βρούμε ρητό a/q τέτοιον ώστε

$$1 \leqslant q \leqslant P^{k-\nu}, \qquad (a,q) = 1,$$

και

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{qP^{k-\nu}} \leqslant \min\left\{\frac{1}{P^{k-\nu}}, \frac{1}{q^2}\right\}.$$

Αν $\alpha \in \Updownarrow$, τότε $\alpha \notin \mathcal{M}(1,0) \cup \mathcal{M}(1,1)$, άρα

$$\frac{1}{P^{k-\nu}} < \alpha < 1 - \frac{1}{P^{k-\nu}}.$$

Επίσης από την αρχική ανισότητα έπεται

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{P^{k-\nu}}$$

και συνεπώς

$$\alpha - \frac{a}{q} \geq -\frac{1}{P^{k-\nu}},$$

δηλαδή

$$\frac{a}{q} \leqslant \alpha + \frac{1}{P^{k-\nu}} < 1$$

και άρα $1 \leqslant a \leqslant q-1$. Αν $q \leqslant P^\nu$, τότε πάλι από την

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{P^{k-\nu}}$$

συμπεραίνουμε ότι

$$\alpha \in \mathcal{M}(q,a) \subseteq \mathcal{M} = [0,1] \setminus \Updownarrow,$$

το οποίο είναι άτοπο. Συνεπώς,

$$P^\nu < q \leqslant P^{k-\nu}.$$

Θέτουμε

$$K = 2^{k-1}. \tag{1.4.1}$$

Από την ανισότητα του Weyl (Θεώρημα **;;**) για την $f(x) = \alpha x^k$ έπεται ότι

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

Εφαρμόζοντας το λήμμα του Hua (Θεώρημα ;;) παίρνουμε

$$\begin{aligned}\Big|\int_{\mathfrak{U}} F(\alpha)^s e(-n\alpha)\,d\alpha\Big| &= \Big|\int_{\mathfrak{U}} F(\alpha)^{s-2^k}F(\alpha)^{2^k} e(-n\alpha)\,d\alpha\Big| \\ &\leqslant \int_{\mathfrak{U}} |F(\alpha)|^{s-2^k}|F(\alpha)|^{2^k}\,d\alpha \\ &\leqslant \max_{\alpha\in\mathfrak{U}}|F(\alpha)|^{s-2^k}\int_0^1 |F(\alpha)|^{2^k}\,d\alpha \\ &\ll (P^{1+\varepsilon-\nu/K})^{s-2^k}P^{2^k-k+\varepsilon} \\ &= P^{s-k-\delta_1},\end{aligned}$$

όπου

$$\delta_1 = \frac{\nu(s-2^k)}{K} - (s-2^k+1)\varepsilon > 0$$

αν το $\varepsilon > 0$ επιλεγεί αρκετά μικρό. Αυτό ολοκληρώνει την απόδειξη. □

1.5 Τα μείζονα τόξα

Ορίζουμε τις βοηθητικές συναρτήσεις

$$v(\beta) = \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m)$$

και

$$S(q,a) = \sum_{r=1}^{q} e(ar^k/q).$$

Θα δείξουμε ότι αν ο α βρίσκεται στο μείζον τόξο $\mathcal{M}(q,a)$ τότε ο $F(\alpha)$ είναι το γινόμενο των $S(q,a)/q$ και $v(\alpha - a/q)$ συν κάποιο μικρό όρο σφάλματος. Αρχικά θα δώσουμε εκτιμήσεις γι΄ αυτές τις συναρτήσεις.

Η ανισότητα $|S(q,a)| \leqslant q$ είναι απλή. Από την ανισότητα του Weyl (θεώρημα ;;) έχουμε

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

άρα

$$\frac{S(q,a)}{q} \ll q^{-\frac{1}{K}+\varepsilon}, \tag{1.5.1}$$

με την σταθερά που υπεισέρχεται σε αυτήν την ανισότητα να εξαρτάται μόνο από το ε.

Λήμμα 1.5.1. *Αν $|\beta| \leqslant 1/2$, τότε*

$$v(\beta) \ll \min\{P, |\beta|^{-1/k}\}.$$

Απόδειξη. Η συνάρτηση $f(x) = \frac{1}{k}x^{\frac{1}{k}-1}$ είναι θετική, συνεχής και φθίνουσα στο $[1,\infty)$. Από το Λήμμα ;; έπεται ότι

$$\begin{aligned}|v(\beta)| &\leqslant \sum_{m=1}^{N}\frac{1}{k}m^{\frac{1}{k}-1} \leqslant \int_1^N \frac{1}{k}x^{\frac{1}{k}-1}dx + f(1) = N^{\frac{1}{k}} - 1 + \frac{1}{k} \\ &< N^{\frac{1}{k}} \leqslant 2\lfloor N^{\frac{1}{k}}\rfloor = 2P.\end{aligned}$$

Αν $|\beta| \leqslant 1/N$ τότε $P \leqslant N^{\frac{1}{k}} \leqslant |\beta|^{-\frac{1}{k}}$ και

$$v(\beta) \ll \min\{P.|\beta|^{-\frac{1}{k}}\}.$$

Υποθέτουμε τώρα ότι $1/N < |\beta| \leqslant 1/2$. Τότε, $|\beta|^{-\frac{1}{k}} \ll P$. Θέτουμε $M = \lfloor |\beta|^{-1} \rfloor$. Τότε,

$$M \leqslant \frac{1}{|\beta|} < M + 1 \leqslant N.$$

Ορίζουμε $U(t) = \sum_{m \leqslant t} e(\beta m)$. Από το Λήμμα **;;** έχουμε $U(t) \leqslant \|\beta\|^{-1} = |\beta|^{-1}$. Αθροίζοντας κατά μέρη (Θεώρημα **;;**) βλέπουμε ότι

$$\sum_{m=M+1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) = f(N)U(N) - f(M)U(M) - \int_M^N U(t) f'(t)\, dt.$$

Έχουμε

$$|f(N)U(N)| = |\frac{1}{k} N^{\frac{1}{k}-1} U(N)| \leqslant \frac{1}{k} N^{\frac{1}{k}-1} |\beta|^{-1} \leqslant \frac{1}{k} \frac{M^{\frac{1}{k}-1}}{|\beta|} \leqslant \frac{1}{k} |\beta|^{-\frac{1}{k}}$$

Ομοίως συνάγουμε ότι

$$|f(M)U(M)| \leqslant \frac{1}{k} \frac{M^{\frac{1}{k}-1}}{|\beta|} \leqslant \frac{1}{k} |\beta|^{-\frac{1}{k}}.$$

Επίσης,

$$\begin{aligned} \left| \int_M^N U(t) f'(t)\, dt \right| &\leqslant \int_M^N |U(t) f'(t)|\, dt \leqslant |\beta|^{-1} \int_M^N |f'(t)|\, dt \\ &= |\beta|^{-1} \frac{1}{k} \left(M^{\frac{1}{k}-1} - N^{\frac{1}{k}-1} \right) \leqslant \frac{1}{k} \frac{M^{\frac{1}{k}-1}}{|\beta|} \leqslant \frac{1}{k} |\beta|^{-\frac{1}{k}} \end{aligned}$$

Δείξαμε λοιπόν ότι

$$\left| \sum_{m=M+1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \right| \leqslant \frac{3}{k} |\beta|^{-\frac{1}{k}}$$

Χρησιμοποιώντας πάλι την μονοτονία της f συμπεραίνουμε όπως πριν ότι

$$\left| \sum_{m=1}^{M} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \right| \leqslant \sum_{m=1}^{M} \frac{1}{k} m^{\frac{1}{k}-1} \leqslant \int_1^M \frac{1}{k} x^{\frac{1}{k}-1} dx + f(1) < M^{\frac{1}{k}} \leqslant |\beta|^{-\frac{1}{k}}$$

Συνεπώς, με χρήση της τριγωνικής ανισότητας προκύπτει ότι

$$\begin{aligned} |v(\beta)| &= |\sum_{m=1}^{M} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) + \sum_{m=M+1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m)| \\ &\leqslant \left| \sum_{m=M+1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \right| + \left| \sum_{m=1}^{M} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \right| \\ &\leqslant \left(1 + \frac{3}{k} \right) |\beta|^{-\frac{1}{k}}. \end{aligned}$$

Αυτό αποδεικνύει το λήμμα. □

Λήμμα 1.5.2. *Έστω q και α ακέραιοι τέτοιοι ώστε $1 \leqslant q \leqslant P^\nu$, $0 \leqslant \alpha \leqslant q$, και $(a,q)=1$. Αν $\alpha \in \mathcal{M}(q,a)$, τότε*

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

Απόδειξη. Θέτουμε $\beta = \alpha - a/q$. Τότε $|\beta| \leqslant P^{\nu-k}$ καθώς $\alpha \in \mathcal{M}(q,a)$ και

$$\begin{aligned} F(\alpha) - \frac{S(q,a)}{q} v(\beta) &= \sum_{m=1}^{P} e(\alpha m^k) - \frac{S(q,a)}{q} \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \\ &= \sum_{m=1}^{P} e\Big(\frac{am^k}{q}\Big) e(\beta m^k) - \frac{S(q,a)}{q} \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \\ &= \sum_{m=1}^{N} u(m) e(\beta m), \end{aligned}$$

όπου

$$u(m) = e(am/q) - \frac{S(q,a)}{q} \frac{1}{k} m^{\frac{1}{k}-1} \quad \text{αν ο } m \text{ είναι } k-\text{οστή δύναμη}$$

και

$$u(m) = -\frac{S(q,a)}{q} \frac{1}{k} m^{\frac{1}{k}-1} \ \text{ αλλιώς.}$$

Θα εκτιμήσουμε το τελευταίο άθροισμα. Κάνουμε την εξής παρατήρηση, εάν $m = lq + r$ για l, r ακεραίους έπεται ότι

$$e(am^k/q) = e\big(a(lq+r)^k/q\big) = e(\ell + ar^k/q) = e(\ell) e(ar^k/q) = e(ar^k/q),$$

καθώς

$$\ell = \frac{a \sum_{n=1}^{k} \binom{k}{n} (lq)^n r^{k-n}}{q} \in \mathbb{Z}.$$

Έστω $y \geqslant 1$. Από την προηγούμενη παρατήρηση και αφού $|S(q,a)| \leqslant q$, έχουμε

$$\begin{aligned} \sum_{1 \leqslant m \leqslant y} e(am^k/q) &= \sum_{r=1}^{q} e(ar^k/q) \sum_{\substack{1 \leqslant m \leqslant y \\ m \equiv r \,(\mathrm{mod}\ q)}} \mathbf{1} \\ &= S(q,a)\Big(\frac{y}{q} + O(1)\Big) \\ &= y \cdot \frac{S(q,a)}{q} + O(q). \end{aligned}$$

Από την μονοτονία της f έχουμε

$$\sum_{k=1}^{t} f(k) - \int_1^t f(k)\, dk \leqslant max(f(1), f(t)) = f(1) = \frac{1}{k}$$

και άρα

$$\sum_{1 \leqslant m \leqslant t} \frac{1}{k} m^{\frac{1}{k}-1} \leqslant t^k - 1 + \frac{1}{k}$$

Έστω $t \geqslant 1$. Από τα παραπάνω έχουμε

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

Αθροίζοντας κατά μέρη παίρνουμε

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

και έχουμε το ζητούμενο. □

Θεώρημα 1.5.3. *Έστω*

$$\mathcal{G}(N,Q) = \sum_{1 \leqslant q \leqslant Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \Big(\frac{S(q,a)}{q}\Big)^s e(-Na/q)$$

και

$$J^*(N) = \int_{P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-N\beta)\,d\beta.$$

Έστω $\mathcal{M}$ το σύνολο των μειζόνων τόξων. Τότε,

$$\int_{\mathcal{M}} F(\alpha)^s e(-N\alpha)\,d\alpha = \mathcal{G}(N,P^\nu)J^*(N) + O(P^{s-k-\delta_2}),$$

όπου $\delta_2 = (1-5\nu) > 0$.

Απόδειξη. Έστω $\alpha \in \mathcal{M}(q,a)$ και

$$\beta = \alpha - \frac{a}{q}.$$

Θέτουμε

$$V = V(\alpha,q,a) = \frac{S(q,a)}{q} v(\alpha - a/q) = \frac{S(q,a)}{q} v(\beta).$$

Αφού $|S(q,a)| \leqslant q$, έχουμε $|V| \ll |v(\beta)| \ll P$ από το Λήμμα 1.5.1. Θέτουμε $F = F(\alpha)$. Τότε, $|F| \leqslant P$. Αφού $F - V = O(P^{2\nu})$ από το Λήμμα 1.5.2, έπεται ότι

$$\begin{aligned} F^s - V^s &= (F-V)(F^{s-1} + F^{s-2}V + \cdots + V^{s-1}) \\ &\ll P^{2\nu}P^{s-1} \\ &= P^{s-1+2\nu}. \end{aligned}$$

Αφού $\mu(\mathcal{M}) \ll P^{3\nu-k}$ από την (1.3.4), έπεται ότι

$$\left| \int_{\mathcal{M}} F(\alpha)^s - V(\alpha)^s e(-N\alpha)\, d\alpha \right| \leqslant \int_{\mathcal{M}} |F^s - V^s|\, d\alpha \ll P^{3\nu-k}P^{s-1+2\nu} = P^{s-k-\delta_2},$$

όπου $\delta_2 = 1 - 5\nu > 0$. Συνεπώς,

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

Για $q \geqslant 2$ έχουμε

$$\begin{aligned} \int_{\mathcal{M}(q,a)} V(\alpha,q,a)^s e(-N\alpha)\, d\alpha &= \int_{a/q-P^{\nu-k}}^{a/q+P^{\nu-k}} V(\alpha,q,a)^s e(-N\alpha)\, d\alpha \\ &= \int_{-P^{\nu-k}}^{P^{\nu-k}} V(\beta+a/q.q,a)^s e(-N(\beta+a/q))\, d\beta \\ &= \Big(\frac{S(q,a)}{q}\Big)^s e(-Na/q) \int_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-N\beta)\, d\beta \\ &= \Big(\frac{S(q,a)}{q}\Big)^s e(-Na/q) J^*(N). \end{aligned}$$

Για $q = 1$ έχουμε $V(\alpha,1,0) = v(\alpha)$ και $V(\alpha,1,1) = v(\alpha-1)$. Άρα,

$$\begin{aligned} &\int_{\mathcal{M}(1,0)} V(\alpha,q,a)^s e(-N\alpha)\, d\alpha + \int_{\mathcal{M}(1,1)} V(\alpha,q,a)^s e(-N\alpha)\, d\alpha \\ &\qquad = \int_0^{P^{\nu-k}} v(\alpha)^s e(-N\alpha)\, d\alpha + \int_{1-P^{\nu-k}}^{1} v(\alpha-1)^s e(-N\alpha)\, d\alpha \\ &\qquad = \int_0^{P^{\nu-k}} v(\beta)^s e(-N\beta)\, d\beta + \int_{-P^{\nu-k}}^{0} v(\beta)^s e(-N\beta)\, d\beta \\ &\qquad = J^*(N). \end{aligned}$$

Συνεπώς,

$$\begin{aligned} \int_{\mathcal{M}} F(\alpha)^s e(-N\alpha)\, d\alpha &= \sum_{1\leqslant q\leqslant P^\nu} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \Big(\frac{S(q,a)}{q}\Big)^s e(-Na/q) J^*(N) + O(P^{s-k-\delta_2}) \\ &= \mathcal{G}(N,P^\nu) J^*(N) + O(P^{s-k-\delta_2}), \end{aligned}$$

και έχουμε το θεώρημα. □

1.6 Το ιδιάζον ολοκλήρωμα

Στη συνέχεια θεωρούμε το ολοκλήρωμα

$$J(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta N)\, d\beta. \tag{1.6.1}$$

Αυτό είναι το *ιδιάζον ολοκλήρωμα* για το πρόβλημα του Waring.

Θεώρημα 1.6.1. *Υπάρχει σταθερά $\delta_3 > 0$ τέτοια ώστε*

$$J(N) \ll P^{s-k}$$

και

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

Απόδειξη. Αρχικά παρατηρούμε ότι η συνάρτηση $g(\beta) = \min\{P.|\beta|^{-1/k}\}^s \geq 0$ είναι άρτια, συνεπώς έχουμε

$$\int_{-1/2}^{1/2} \min\{P.|\beta|^{-1/k}\}^s\, d\beta = 2\int_0^{1/2} \min\{P.|\beta|^{-1/k}\}^s\, d\beta$$

Από αυτό σε συνδυασμό με το Λήμμα 1.5.1 έχουμε

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

Υπολογίζοντας τα ολοκληρώματα έχουμε

$$\int_0^{1/N} P^s\, d\beta = \frac{P^s}{N} = \frac{P^s}{(N^{1/k})^k} \leqslant \frac{P^s}{P^k} = P^{s-k}$$

και

$$\left| \int_{1/N}^{1/2} \beta^{-s/k}\, d\beta \right| = \left| \frac{2^{\frac{s}{k}-1} - N^{\frac{s}{k}-1}}{-\frac{s}{k}+1} \right| = \frac{s-k}{k}(N^{\frac{s}{k}-1} - 2^{\frac{s}{k}-1}) \leqslant \frac{s-k}{k}(N^{\frac{s-k}{k}}) \ll P^{s-k}.$$

Από τα παραπάνω έπεται ότι

$$J(N) \ll P^{s-k}.$$

Επιπλέον έχουμε

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

όπου $\delta_3 = \nu(s/k-1) > 0$. □

Λήμμα 1.6.2. *Έστω α και β πραγματικοί αριθμοί τέτοιοι ώστε $0 < \beta < 1$ και $\alpha \geqslant \beta$. Τότε,*

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

με την σταθερά (στο O) να εξαρτάται μόνο από το β.

Απόδειξη. Η συνάρτηση

$$g(x) = x^{\beta-1}(N-x)^{\alpha-1}$$

είναι θετική και συνεχής στο $(0,N)$, ολοκληρώσιμη στο $[0,N]$, και

$$\begin{aligned} \int_0^N g(x)\, dx &= \int_0^N x^{\beta-1}(N-x)^{\alpha-1} dx \\ &= N^{\alpha+\beta-1}\int_0^1 t^{\beta-1}(1-t)^{\alpha-1} dt \\ &= N^{\alpha+\beta-1} B(\alpha,\beta) \\ &= N^{\alpha+\beta-1}\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}, \end{aligned}$$

όπου $B(\alpha,\beta)$ είναι η συνάρτηση Βήτα και $\Gamma(\alpha)$ είναι η συνάρτηση Γάμμα.

Αν $\alpha \geqslant 1$, τότε

$$g'(x) = g(x)\Big(\frac{\beta-1}{x} - \frac{\alpha-1}{N-x}\Big) < 0,$$

άρα η $g(x)$ είναι φθίνουσα στο $(0,N)$ και

$$\int_1^N g(x)\, dx < \sum_{m=1}^{N-1} g(m) < \int_0^{N-1} g(x)\, dx.$$

Συνεπώς,

$$\begin{aligned}
0 &< \int_{N-1}^{N} g(x)\,dx + \left(\int_0^{N-1} g(x)\,dx - \sum_{m=1}^{N-1} g(m)\right)\\
&= \int_0^N g(x)\,dx - \sum_{m=1}^{N-1} g(m)\\
&= \int_0^1 g(x)\,dx + \left(\int_1^N g(x)\,dx - \sum_{m=1}^{N-1} g(m)\right)\\
&< \int_0^1 g(x)\,dx\\
&= \int_0^1 x^{\beta-1}(N-x)^{\alpha-1}dx\\
&\leqslant N^{\alpha-1}\int_0^1 x^{\beta-1}dx\\
&= \frac{N^{\alpha-1}}{\beta}.
\end{aligned}$$

Αν $0 < \beta \leqslant \alpha < 1$, τότε $0 < \alpha + \beta < 2$ και είναι έυκολο να ελέγξουμε ότι η $g(x)$ έχει τοπικό ελάχιστο στο

$$c = \frac{(1-\beta)N}{2-\alpha-\beta} \in [N/2, N).$$

Αφού η $g(x)$ είναι γνησίως φθίνουσα στο $(0, c)$, έπεται ότι

$$\sum_{m=1}^{\lfloor c\rfloor} g(m) < \int_0^{\lfloor c\rfloor} g(x)\,dx < \int_0^c g(x)\,dx$$

και

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

όπου στην τελευταία ανισότητα χρησιμοποιήσαμε την σχέση

$$\int_0^1 g(x)\,dx < \frac{N^{\alpha-1}}{\beta}.$$

Όμοια, αφού η $g(x)$ είναι αύξουσα στο (c, N), έπεται ότι

$$\sum_{m=\lfloor c\rfloor+1}^{N-1} g(m) \leqslant \int_{\lfloor c\rfloor+1}^{N} g(x)\,dx < \int_{c}^{N} g(x)\,dx$$

και

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

όπου η τελευταία ανισότητα προκύπτει από το ότι

$$\int_{N-1}^{N} g(x)\,dx = \int_{N-1}^{N} x^{\beta-1}(N-x)^{\alpha-1}dx = \int_{0}^{1} (N-t)^{\beta-1}t^{\alpha-1}dt$$

Συνεπώς,

$$0 < \int_{0}^{N} g(x)\,dx - \sum_{m=1}^{N-1} g(m) < \frac{N^{\alpha-1}}{\beta} + \frac{N^{\beta-1}}{\alpha} \leqslant \frac{2N^{\alpha-1}}{\beta},$$

όπως θέλαμε. □

Θεώρημα 1.6.3. *Αν $s \geqslant 2$ τότε*

$$J(N) = \Gamma\Big(1+\frac{1}{k}\Big)^{s}\Gamma\Big(\frac{s}{k}\Big)^{-1}N^{s/k-1} + O(N^{(s-1)/k-1}).$$

Απόδειξη. Ορίζουμε

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

για $s \geqslant 1$. Θα υπολογίσουμε αυτό το ολοκλήρωμα με επαγωγή ως προς s. Από την

$$v(\beta) = \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m)$$

βλέπουμε ότι

$$v(\beta)^s = \frac{1}{k^s}\sum_{m_1=1}^{N}\cdots\sum_{m_s=1}^{N}(m_1\cdots m_s)^{\frac{1}{k}-1}e((m_1+\cdots+m_s)\beta),$$

άρα

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

Ειδικότερα, για $s = 2$, εφαρμόζουμε το Λήμμα 1.6.2 με $\alpha = \beta = 1/k$ και παίρνουμε

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

Έτσι έχουμε το ζητούμενο στην περίπτωση $s = 2$.

Αν $s \geqslant 2$ και το θεώρημα ισχύει για τον s, γράφουμε

$$\begin{aligned} J_{s+1}(N) &= \int_{-1/2}^{1/2} v(\beta)^{s+1} e(-N\beta)\, d\beta \\ &= \int_{-1/2}^{1/2} v(\beta) v(\beta)^s e(-N\beta)\, d\beta \\ &= \int_{-1/2}^{1/2} \sum_{k=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) v(\beta)^s e(-N\beta)\, d\beta \\ &= \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} \int_{-1/2}^{1/2} v(\beta)^s e(-(N-m)\beta)\, d\beta \\ &= \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} J_s(N-m) \\ &= \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} \sum_{m=1}^{N-1} \frac{1}{k} m^{\frac{1}{k}-1} (N-m)^{\frac{s}{k}-1} \\ &\qquad + O\Big(\sum_{m=1}^{N-1} \frac{1}{k} m^{\frac{1}{k}-1} (N-m)^{\frac{s-1}{k}-1} \Big). \end{aligned}$$

Εφαρμόζοντας το Λήμμα 1.6.2 στον κύριο όρο (με $\alpha = s/k$ και $\beta = 1/k$) και στο σφάλμα (με $\alpha = (s-1)/k$ και $\beta = 1/k$), παίρνουμε

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

και

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

Άρα,

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

και έχουμε ολοκληρώσει το επαγωγικό βήμα. □

1.7 Η ιδιάζουσα σειρά και το θεώρημα των Hardy και Littlewood

Στο Θεώρημα 1.5.3 ορίσαμε την συνάρτηση

$$\mathcal{G}(N,Q) = \sum_{1\leqslant q\leqslant Q} A_N(q),$$

όπου

$$A_N(q) = \sum_{\substack{a=1\\(a,q)=1}}^{q} \Big(\frac{S(q,a)}{q}\Big)^s e(-Na/q).$$

Ορίζουμε τώρα την *ιδιάζουσα σειρά* για το πρόβλημα του Waring: είναι η αριθμητική συνάρτηση

$$\mathcal{G}(N) = \sum_{q=1}^{\infty} A_N(q).$$

Για κάθε $0<\varepsilon<\frac{1}{sK}$, από την $s\geqslant 2^k+1 = 2K+1$ έχουμε

$$\frac{s}{K} - 1 - s\varepsilon \geqslant 1 + \frac{1}{K} - s\varepsilon = 1+\delta_4,$$

όπου

$$\delta_4 = \frac{1}{K} - s\varepsilon > 0.$$

Από την (1.5.1) βλέπουμε ότι

$$A_N(q) \ll \frac{q}{q^{\frac{s}{K}-s\varepsilon}} \leqslant \frac{1}{q^{1+\delta_4}}, \tag{1.7.1}$$

άρα η ιδιάζουσα σειρά $\sum_q A_N(q)$ συγκλίνει απολύτως και ομοιόμορφα ως προς N. Ειδικότερα, υπάρχει σταθερά $c_2 = c_2(k,s)$ τέτοια ώστε

$$|\mathcal{G}(N)| < c_2 \tag{1.7.2}$$

για όλους τους φυσικούς N. Επιπλέον,

$$\mathcal{G}(N) - \mathcal{G}(N,P^\nu) = \sum_{q>P^\nu} A_N(a) \ll \sum_{q>P^\nu}\frac{1}{q^{1+\delta_4}} \ll P^{-\nu\delta_4},$$

διότι

$$\sum_{q>P^\nu}\frac{1}{q^{1+\delta_4}} = \sum_{q=1}^{\infty}\frac{1}{q^{1+\delta_4}} - \sum_{q=1}^{P^\nu}\frac{1}{q^{1+\delta_4}} \leqslant c - \frac{P^\nu}{P^{\nu(1+\delta 4)}} = c - P^{-\nu\delta 4},$$

όπου

$$c = \sum_{q=1}^{\infty} \frac{1}{q^{1+\delta_4}} \in \mathbb{R}$$

Θα δείξουμε ότι $\mathcal{G}(N) > 0$ για κάθε N και ότι υπάρχει σταθερά $c_1 > 0$, που εξαρτάται μόνο από τους k και s, τέτοια ώστε

$$0 < c_1 < \mathcal{G}(N) < c_2$$

για όλους τους φυσικούς N. Αρχίζουμε δείχνοντας ότι η $A_N(q)$ είναι πολλαπλασιαστική συνάρτηση του q. Η επόμενη απλή παρατήρηση θα φανεί χρήσιμη.

Λήμμα 1.7.1. *Έστω $(q,r) = 1$. Τότε κάθε κλάση ισοτιμίας $\bmod\ qr$ γράφεται μονοσήμαντα στη μορφή $xr + yq$, όπου $1 \leqslant x \leqslant q$ και $1 \leqslant y \leqslant r$.*

Απόδειξη. Έστω A το σύνολο των κλάσεων ισοτιμίας $\bmod\ qr$ και $B = \{xr + yq : 1 \leqslant x \leqslant q, 1 \leqslant y \leqslant r\}$. Ορίζουμε την συνάρτηση f από το B στο A με

$$f(xr + yq) = [xr + yq].$$

Θα δείξουμε ότι είναι $1-1$ και επί. Τα σύνολα A,B έχουν την ίδια πληθικότητα συνεπώς αρκεί να δείξουμε ότι η f είναι $1-1$. Προς τούτο έστω $xr + yq, x'r + y'q$ με

$$f(xr + yq) = f(x'r + y'q.)$$

Δηλαδή

$$xr + yq \equiv x'r + y'q \pmod{qr}$$

και άρα

$$(x - x')r \equiv (y - y')q \pmod{qr}.$$

Από την σχέση αυτή πολλαπλασιάζοντας με r προκύπτει ότι

$$(x - x')r^2 \equiv (y - y')qr \pmod{qr}$$

το οποίο σημαίνει ότι ο q διαιρεί τον $(x - x')r^2$ και καθώς $(q,r) = 1$ συμπεραίνουμε ότι ο q διαιρεί τον $x - x'$. Έτσι $x = x'$. Με όμοιο τρόπο δείχνουμε ότι $y = y'$. Συνεπώς $xr + yq = x'r + y'q$ και η απόδειξη ολοκληρώθηκε. □

Λήμμα 1.7.2. *Έστω $(q,r) = 1$. Τότε κάθε αντιστρέψιμη κλάση ισοτιμίας $\pmod{qr}$ γράφεται μονοσήμαντα στην μορφή $ar + bq$, όπου $1 \leqslant a \leqslant q$, $1 \leqslant b \leqslant r$ και $(a,q) = (b,r) = 1$.*

Απόδειξη. Έστω C το σύνολο των αντιστρέψιμων κλάσεων ισοτιμίας $\bmod\ qr$ και $D = \{ar + bq : 1 \leqslant a \leqslant q, 1 \leqslant b \leqslant r, (a,q) = (b,r) = 1\}$. Ορίζουμε την συνάρτηση g από το D στο C με

$$g(ar + bq) = [ar + bq].$$

Θα δείξουμε ότι είναι $1-1$ και επί. Αρχικά δείχνουμε ότι η g ορίζεται καλά. Αρκεί να δείξουμε ότι αν $c = ar + bq$ όπου $(a,q) = (b,r) = 1$ τότε $(c,qr) = 1$. Έστω πρώτος p ο οποίος διαιρεί τον (c,qr). Τότε καθώς $(q,r) = 1$ συμπεραίνουμε ότι ο p δεν διαιρεί ταυτόχρονα τους q,r. Έστω χωρίς

βλάβη της γενικότητας ότι $p|q$. Τότε καθώς $p|(ar+bq)=c$ και $p|bq$ προκύπτει ότι $p|ar$. Άρα αφού ο ο p δεν διαιρεί τον r έπεται ότι $p|a$ και συνεπώς $p|(a,q)=1$, άτοπο. Έτσι $(c,qr)=1$. Επίσης,

$$|C| = \varphi(qr) = \varphi(q)\varphi(r) = |d|,$$

καθώς η συνάστηση φ του Euler είναι πολλαπλασιαστική. όμοια με το προηγούμενο λήμμα η g είναι $1-1$ άρα και επί. Η απόδειξη ολοκληρώθηκε. □

Λήμμα 1.7.3. *Έστω* $(q,r)=1$. *Τότε,*

$$S(qr, ar+bq) = S(q,a)S(r,b).$$

Απόδειξη. Αφού $(q,r)=1$, τα σύνολα $\{xr : 1 \leqslant x \leqslant q\}$ και $\{yq : 1 \leqslant y \leqslant r\}$ είναι πλήρη συστήματα υπολοίπων mod q και r, αντίστοιχα. Αφού κάθε κλάση ισοτιμίας mod qr γράφεται μονοσήμαντα στη μορφή $xr+yq$, όπου $1 \leqslant x \leqslant q$ και $1 \leqslant y \leqslant r$, έπεται ότι

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

και έχουμε το λήμμα. □

Λήμμα 1.7.4. *Αν* $(q,r)=1$, *τότε*

$$A_N(qr) = A_N(q)A_N(r).$$

Δηλαδή, η συνάρτηση A_N *είναι πολλαπλασιαστική.*

Απόδειξη. Αν οι c και qr είναι σχετικώς πρώτοι, τότε ο c είναι ισότιμος mod qr με κάποιον αριθμό

της μορφής $ar + bq$, όπου $(a, q) = (b, r) = 1$. Από το Λήμμα 1.7.3 προκύπτει ότι

$$\begin{aligned} A_N(qr) &= \sum_{\substack{c=1\\(c,qr)=1}}^{qr} \Big(\frac{S(qr,c)}{qr}\Big)^s e\Big(-\frac{cN}{qr}\Big) \\ &= \sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{\substack{b=1\\(b,q)=1}}^{r} \Big(\frac{S(qr,ar+bq)}{qr}\Big)^s e\big(-\frac{(ar+bq)N}{qr}\Big) \\ &= \sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{\substack{b=1\\(b,q)=1}}^{r} \Big(\frac{S(q,a)}{q}\Big)^s \Big(\frac{S(r,b)}{r}\Big)^s e\Big(-\frac{aN}{q}\Big)e\Big(-\frac{bN}{r}\Big) \\ &= \sum_{\substack{a=1\\(a,q)=1}}^{q} \Big(\frac{S(q,a)}{q}\Big)^s e\Big(-\frac{aN}{q}\Big) \sum_{\substack{b=1\\(b,q)=1}}^{r} \Big(\frac{S(r,b)}{r}\Big)^s e\Big(-\frac{bN}{r}\Big) \\ &= A_N(q)A_N(r), \end{aligned}$$

και έχουμε το ζητούμενο. □

Για κάθε φυσικό αριθμό q, συμβολίζουμε με $M_N(q)$ το πλήθος των λύσεων της ισοτιμίας

$$x_1^k + \cdots + x_s^k \equiv N \pmod{q}$$

πάνω από τους ακεραίους x_i που ικανοποιούν την $1 \leqslant x_i \leqslant q$ για $i = 1, \ldots, q$.

Λήμμα 1.7.5. *Έστω $s \geqslant 2^k + 1$. Για κάθε πρώτο p, η σειρά*

$$\chi_N(p) = 1 + \sum_{h=1}^{\infty} A_N(p^h) \tag{1.7.3}$$

συγκλίνει, και

$$\chi_N(p) = \lim_{h\to\infty} \frac{M_N(p^h)}{p^{h(s-1)}}. \tag{1.7.4}$$

Απόδειξη. Η σύγκλιση της σειράς (1.7.3) είναι άμεση συνέπεια της ανισότητας (1.7.1). Αν $(a, q) = d$ τότε

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

Αν $m \equiv 0 \pmod{q}$ τότε

$$\frac{1}{q}\sum_{a=1}^{q} e\Big(\frac{am}{q}\Big) = \frac{1}{q}q = 1$$

καθώς για κάθε a ο αριθμός $\frac{am}{q}$ είναι ακέραιος. Εάν ο q δεν διαιρεί τον m τότε $e\Big(\frac{m}{q}\Big) \neq 1$ και συνεπώς

$$\sum_{a=1}^{q} e\Big(\frac{am}{q}\Big) = \sum_{a=0}^{q} e\Big(\frac{m}{q}\Big)^a - e\Big(\frac{m}{q}\Big)^0 = \frac{e(m/q)^{q+1} - 1}{e(m/q) - 1} - 1 = \frac{e(m/q)^{q+1} - e(m/q)}{e(m/q) - 1} = 0$$

αφού $e(m/q)^{q+1} = e(m/q)$. Έπεται δηλαδή ότι το άθροισμα

$$\frac{1}{q}\sum_{a=1}^{q} e\Big(\frac{am}{q}\Big)$$

είναι ίσο με 1 αν $m \equiv 0 \pmod q$ και ίσο με 0 αλλιώς, βλέπουμε ότι για οποιουσδήποτε ακεραίους $x_1, \dots, x_s$ το άθροισμα

$$\frac{1}{q}\sum_{a=1}^{q} e\Big(\frac{a(x_1^k + \cdots + x_s^k - N)}{q}\Big)$$

είναι ίσο με 1 αν $x_1^k + \cdots + x_s^k \equiv N \pmod q$ και ίσο με 0 αλλιώς. Άρα,

$$\begin{aligned}
M_N(q) &= \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} \frac{1}{q}\sum_{a=1}^{q} e\Big(\frac{a(x_1^k + \cdots + x_s^k - N)}{q}\Big) \\
&= \frac{1}{q}\sum_{a=1}^{q}\sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} e\Big(\frac{a(x_1^k + \cdots + x_s^k - N)}{q}\Big) \\
&= \frac{1}{q}\sum_{a=1}^{q}\sum_{x_1=1}^{q} e\Big(\frac{ax_1^k}{q}\Big) \cdots \sum_{x_s=1}^{q} e\Big(\frac{ax_s^k}{q}\Big) e\Big(-\frac{aN}{q}\Big) \\
&= \frac{1}{q}\sum_{a=1}^{q} S(q,a)^s e\Big(-\frac{aN}{q}\Big) \\
&= \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1\\(a,q)=d}}^{q} S(q,a)^s e\Big(-\frac{aN}{q}\Big) \\
&= \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1\\(a,q)=d}}^{q} d^s S\Big(\frac{q}{d}, \frac{a}{d}\Big)^s e\Big(-\frac{(a/d)N}{q/d}\Big) \\
&= \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1\\(a,q)=d}}^{q} q^s \Big(\frac{S(q/d, a/d)}{q/d}\Big)^s e\Big(-\frac{(a/d)N}{q/d}\Big) \\
&= q^{s-1}\sum_{d|q} A_N(q/d).
\end{aligned}$$

Συνεπώς,

$$\sum_{d|q} A_N(q/d) = q^{1-s} M_N(q)$$

για κάθε $q \geqslant 1$. Ειδικότερα, για $q = p^h$ παίρνουμε

$$1 + \sum_{j=1}^{h} A_N(p^j) = \sum_{d|p^h} A_N(p^h/d) = p^{h(1-s)} M_N(p^h),$$

άρα

$$\chi_N(p) = \lim_{h\to\infty}\Big(1 + \sum_{j=1}^{h} A_N(p^j)\Big) = \lim_{h\to\infty} p^{h(1-s)} M_N(p^h),$$

και η απόδειξη είναι πλήρης. □

Λήμμα 1.7.6. *Αν $s \geqslant 2^k + 1$, τότε*

$$\mathcal{G}(N) = \prod_p \chi_N(p). \tag{1.7.5}$$

Επιπλέον, υπάρχει σταθερά c_2 που εξαρτάται μόνο από τους k και s, τέτοια ώστε

$$0 < \mathcal{G}(N) < c_2$$

για κάθε N, και υπάρχει πρώτος p_0 που εξαρτάται μόνο από τους k και s, τέτοιος ώστε

$$\frac{1}{2} \leqslant \prod_{p > p_0} \chi_N(p) \leqslant \frac{3}{2} \tag{1.7.6}$$

για κάθε $N \geqslant 1$.

Απόδειξη. Έχουμε δείξει ότι αν $s \geqslant 2^k + 1$ τότε

$$A_N(q) \ll \frac{1}{q^{1+\delta_4}},$$

όπου ο δ_4 εξαρτάται μόνο από τους k και s, άρα η σειρά $\sum_q A_N(q)$ συγκλίνει απολύτως. Αφού η συνάρτηση $A_n(q)$ είναι πολλαπλασιαστική, από το (;;) γνωρίζουμε ότι

$$\mathcal{G}(N) = \sum_{q=1}^{\infty} A_N(q) = \prod_p \Big(1 + \sum_{h=1}^{\infty} A_N(p^h)\Big) = \prod_p \chi_N(p).$$

και άρα και το γινόμενο Euler (1.7.5) συγκλίνει. Ειδικότερα, $\chi_N(p) \neq 0$ για κάθε N και p. Αφού ο $\chi_N(p)$ είναι μη αρνητικός από την (1.7.4), συμπεραίνουμε ότι ο $\chi_N(p)$ είναι θετικός πραγματικός αριθμός για κάθε N και p, συνεπώς η ιδιάζουσα σειρά $\mathcal{G}(N)$ είναι θετική. Πάλι, από την (1.7.1),

$$0 < \mathcal{G}(N) \leqslant \sum_{q=1}^{\infty} \frac{1}{q^{1+\delta_4}} = c_2 < \infty$$

και

$$|\chi_N(p) - 1| \leqslant \sum_{h=1}^{\infty} |A_N(p^h)| \ll \sum_{h=1}^{\infty} \frac{1}{p^{h(1+\delta_4)}} \ll \frac{1}{p^{1+\delta_4}}.$$

Συνεπώς, υπάρχει σταθερά c που εξαρτάται μόνο από τους k και s, τέτοια ώστε

$$1 - \frac{c}{p^{1+\delta_4}} \leqslant \chi_n(p) \leqslant 1 + \frac{c}{p^{1+\delta_4}}$$

για κάθε N και p. Τώρα από το θεώρημα (;;) η σύγκλιση της σειράς $\sum_p \left(\frac{c}{p^{1+\delta 4}}\right)$ συνεπάγεται τη σύγκλιση του άπειρου γινομένου $\prod_p \left(1 + \frac{c}{p^{1+\delta 4}}\right)$. Άρα υπάρχει θετικός πραγματικός αριθμός α με

$$\prod_p \left(1 + \frac{c}{p^{1+\delta 4}}\right) = \alpha > 1,$$

αφού $1 + \frac{c}{p^{1+\delta 4}} > 1$ για κάθε p. Θέτουμε

$$\varepsilon = \frac{\alpha}{3} > 0.$$

Τότε υπάρχει p_1 πρώτος τέτοιος ώστε

$$\prod_{p\leqslant p_1}\left(1+\frac{c}{p^{1+\delta 4}}\right)>\alpha-\frac{\alpha}{3}=\frac{2\alpha}{3}.$$

Έπεται λοιπόν ότι

$$\prod_{p>p_1}\left(1+\frac{c}{p^{1+\delta 4}}\right)=\frac{\prod_p\left(1+\frac{c}{p^{1+\delta 4}}\right)}{\prod_{p\leqslant p_1}\left(1+\frac{c}{p^{1+\delta 4}}\right)}\leqslant\frac{3}{2}.$$

ομοίως βρίσκουμε p_2 τέτοιον ώστε

$$\prod_{p>p_2}\left(1-\frac{c}{p^{1+\delta 4}}\right)\geqslant\frac{1}{2}.$$

Θέτοντας $p_0=\max(p_1,p_2)$ παίρνουμε τη σχέση (1.7.6). □

Θέλουμε να δείξουμε ότι ο $\mathcal{G}(N)$ είναι φραγμένος μακρυά από το 0 ομοιόμορφα ως προς N. Από την ανισότητα (1.7.6), αρκεί να δείξουμε, για κάθε πρώτο p, ότι ο $\chi_N(p)$ είναι ομοιόμορφα φραγμένος μακρυά από το 0.

Έστω p πρώτος, και έστω

$$k=p^r k_0,$$

όπου $r\geqslant 0$ και $(p,k_0)=1$. Ορίζουμε $\gamma:=r+1$ αν $p>2$ και $\gamma:=r+2$ αν $p=2$.

Λήμμα 1.7.7. *Έστω m φυσικός που δεν διαιρείται από τον p. Αν η ισοτιμία $x^k\equiv m\pmod{p^\gamma}$ έχει λύση, τότε η ισοτιμία $y^k\equiv m\pmod{p^h}$ έχει λύση για κάθε $h\geqslant\gamma$.*

Απόδειξη. Διακρίνουμε δύο περιπτώσεις. Ας υποθέσουμε πρώτα ότι ο p είναι περιττός πρώτος. Για $h\geqslant\gamma=r+1$, έχουμε

$$(k,\varphi(p^h))=(k_0p^r,(p-1)p^{h-1})=(k_0,p-1)p^r=(k,\varphi(p^\gamma)).$$

Οι κλάσεις ισοτιμίας mod p^h που είναι σχετικώς πρώτες προς τον p σχηματίζουν κυκλική ομάδα τάξης $\varphi(p^h)=(p-1)p^{h-1}$. Έστω g ένας γεννήτορας αυτής της κυκλικής ομάδας, δηλαδή, μια πρωταρχική ρίζα mod p^h. Τότε, ο g είναι επίσης πρωταρχική ρίζα mod p^γ. Έστω $x^k\equiv m\pmod{p^\gamma}$. Τότε $(x,p)=1$, και μπορούμε να επιλέξουμε ακεραίους r και u τέτοιους ώστε

$$x\equiv g^u\pmod{p^h}$$

και

$$m\equiv g^r\pmod{p^h}.$$

Τότε

$$ku\equiv r\pmod{\varphi(p^\gamma)},$$

άρα

$$r\equiv 0\pmod{(k,\varphi(p^\gamma))}$$

και

$$r\equiv 0\pmod{(k,\varphi(p^h))}.$$

Συνεπώς, υπάρχει ακέραιος v τέτοιος ώστε

$$kv \equiv r \pmod{\varphi(p^h)}.$$

Έστω $y = g^v$. Τότε, $y^k \equiv m \pmod{p^h}$.

Στη δεύτερη περίπτωση, έχουμε $p = 2$ άρα οι m και x είναι περιττοί. Αν $r = 0$ τότε ο k είναι περιττός. Καθώς ο y διατρέχει το σύνολο των περιττών κλάσεων ισοτιμίας mod 2^h, το ίδιο ισχύει για τον y^k, και η ισοτιμία $y^k \equiv m \pmod{2^h}$ έχει λύση για κάθε $h \geqslant 1$. Αν $r \geqslant 1$ τότε ο k είναι άρτιος και $m \equiv x^k \equiv 1 \pmod{4}$. Επίσης, $x^k = (-x)^k$, άρα μπορούμε να υποθέσουμε ότι $x \equiv 1 \pmod{4}$. Οι κλάσεις ισοτιμίας mod 2^h που είναι ισότιμες με $1 \bmod 4$ σχηματίζουν κυκλική υποομάδα τάξης 2^{h-2}, και ο 5 είναι γεννήτορας αυτής της υποομάδας. Επιλέγουμε ακεραίους r και u τέτοιους ώστε

$$m \equiv 5^r \pmod{2^h}$$

και

$$x \equiv 5^u \pmod{2^h}.$$

Τότε, η $x^k \equiv m \pmod{2^\gamma}$ είναι ισοδύναμη με την

$$ku \equiv r \pmod{2^{\gamma-2}},$$

άρα ο r είναι πολλαπλάσιο του $(k, 2^r) = 2^r = (k, 2^{h-2})$. Έπεται ότι υπάρχει ακέραιος v τέτοιος ώστε

$$kv \equiv r \pmod{2^{h-2}}.$$

Έστω $y = 5^v$. Τότε, $y^k \equiv m \pmod{2^h}$, και η απόδειξη είναι πλήρης. □

Λήμμα 1.7.8. *Έστω p πρώτος. Αν υπάρχουν ακέραιοι $a_1, \ldots, a_s$, που δεν διαιρούνται όλοι από τον p, τέτοιοι ώστε*

$$a_1^k + \cdots + a_s^k \equiv N \pmod{p^\gamma},$$

τότε

$$\chi_N(p) \geqslant \frac{1}{p^{\gamma(1-s)}} > 0.$$

Απόδειξη. Υποθέτουμε ότι $a_1 \not\equiv 0 \pmod{p}$. Έστω$h > \gamma$. Για κάθε $i = 2, \ldots, s$ υπάρχουν $p^{h-\gamma}$ ανά δύο όχι ισότιμοι ακέραιοι x_i τέτοιοι ώστε

$$x_i \equiv a_i \pmod{p^h}.$$

Αφού η ισοτιμία

$$x_1^k \equiv N - x_1^k - \cdots - x_s^k \pmod{p^\gamma}$$

έχει λύση $x_1 = a_1 \not\equiv 0 \pmod{p}$, από το Λήμμα 1.7.7 βλέπουμε ότι η

$$x_1^k \equiv N - x_1^k - \cdots - x_s^k \pmod{p^h}$$

έχει λύση. Έπεται ότι

$$M_N(p^h) \geqslant p^{(h-\gamma)(s-1)},$$

άρα

$$\chi_N(p) = \lim_{h\to\infty} \frac{M_N(p^h)}{p^{h(s-1)}} \geqslant \frac{1}{p^{\gamma(s-1)}} > 0.$$

□

Λήμμα 1.7.9. *Αν $s \geqslant 2k$ για περιττό k ή $s \geqslant 4k$ για άρτιο k, τότε*

$$\chi_N(p) \geqslant p^{\gamma(1-s)} > 0.$$

Απόδειξη. Από το Λήμμα 1.7.8 αρκεί να αποδείξουμε ότι η ισοτιμία

$$a_1^k + \cdots + a_{s-1}^k + 1^k \equiv N \pmod{p^\gamma} \tag{1.7.7}$$

έχει λύση στους ακεραίους. Ισοδύναμα, αρκεί να λύσουμε την ισοτιμία

$$a_1^k + \cdots + a_{s-1}^k \equiv N - 1 \pmod{p^\gamma}.$$

Σε αυτήν την περίπτωση έχουμε $(N-1, p) = 1$. Αρκεί λοιπόν να δείξουμε ότι αν $(N, p) = 1$ τότε η ισοτιμία (1.7.7) έχει λύση στους ακεραίους για $s \geqslant 2k-1$ αν ο p είναι περιττός και για $s \geqslant 4k-1$ αν ο p είναι άρτιος.

Έστω p περιττός πρώτος και g μια πρωταρχική ρίζα $\bmod\ p^\gamma$. Η τάξη της g είναι

$$\varphi(p^\gamma) = (p-1)p^{\gamma-1} = (p-1)p^r.$$

Έστω $(m, p) = 1$. Ο ακέραιος m είναι υπόλοιπο k-οστής δύναμης $\bmod\ p^\gamma$ αν και μόνο αν υπάρχει ακέραιος x τέτοιος ώστε

$$x^k \equiv m \pmod{p^\gamma}.$$

Έστω $m \equiv g^r \pmod{p^\gamma}$. Τότε, ο m είναι υπόλοιπο k-οστής δύναμης αν και μόνο αν υπάρχει ακέραιος v τέτοιος ώστε $x \equiv g^v \pmod{p^\gamma}$ και

$$kv \equiv r \pmod{(p-1)p^r}.$$

Αφού $k = k_0 p^r$ με $(k_0, p) = 1$, έπεται ότι η ισοτιμία έχει λύση αν και μόνο αν

$$r \equiv 0 \pmod{(k_0, (p-1)p^r)},$$

υνεπώς υπάρχουν

$$\frac{\varphi(p^\gamma)}{(k_0, p-1)p^r} = \frac{p-1}{(k_0, p-1)}$$

διακεκριμένα υπόλοιπα k-οστών δυνάμεων $\bmod\ p^\gamma$. Έστω $s(N)$ ο μικρότερος φυσικός s για τον οποίο η (1.7.7) έχει λύση, και $C(j)$ το σύνολο όλων των κλάσεων ισοτιμίας $N \bmod p^\gamma$ για τις οποίες $(N, p) = 1$ και $s(N) = j$. Ειδικότερα, το $C(1)$ αποτελείται ακριβώς από τα υπόλοιπα k-οστώ δυνάμεων $\bmod\ p^\gamma$. Αν $(m, p) = 1$ και $N' = m^k N$, τότε $s(N') = s(N)$. Έπεται ότι τα σύνολα $C(j)$ είναι κλειστά ως προς πολλαπλασιασμό με υπόλοιπα k-οστών δυνάμεων, άρα, αν το $C(j)$ είναι μη κενό τότε $|C(j)| \geqslant (p-1)/(k_0, p-1)$. Έστω n ο μεγαλύτερος φυσικός για τον οποίο το σύνολο $C(n)$ είναι μη κενό. Έστω $j < n$ και έστω N ο μικρότερος φυσικός για τον οποίο $(N, p) = 1$ και $s(N) > j$. Αφού ο p είναι περιττός πρώτος, έπεται ότι ο $N - i$ είναι πρώτος προς τον p για $i = 1$ ή 2, και $s(N-i) \leqslant j$. Αφού $N = (N-1) + 1^k$ και $N = (N-2) + 1^k + 1^k$, έπεται ότι

$$j + 1 \leqslant (N) \leqslant s(N-i) + 2 \leqslant j + 2$$

άρα $s(N-i) = j$ ή $j-1$. Αυτό σημαίνει ότι δεν υπάρχουν διαδοχικά μη κενά σύβολα $C(j)$ για $j = 1, 2, \ldots, n$, άρα το πλήθος των μη κενών συνόλων $C(j)$ είναι τουλάχιστον $\frac{n+1}{2}$. Αφού τα σύνολα $C(j)$ είναι ξένα ανά δύο, έπεται ότι

$$(p-1)p^r = \varphi(p^\gamma) = \sum_{\substack{j=1 \\ C(j)\neq\emptyset}}^{n} |C(j)| \geqslant \frac{n+1}{2}\frac{p-1}{(k_0, p-1)},$$

άρα

$$n \leqslant 2(k_0, p-1)p^r - 1 \leqslant 2k-1.$$

Άρα, $s(N) \leqslant 2k-1$ αν ο p είνα περιττός πρώτος και ο N είναι πρώτος προς τον p.

Έστω $p = 2$. Αν ο k είναι περιττός, τότε κάθε περιττός ακέραιος είναι υπόλοιπο k-οστής δύναμης $\bmod\ 2^\gamma$, άρα $s(N) = 1$ για όλους τους περιττούς ακεραίους N. Αν ο k είναι άρτιος, τότε $k = 2^r k_0$ με $r \geqslant 1$ και $\gamma = r+2$. Μπορούμε να υποθέσουμε ότι $1 \leqslant N \leqslant 2^\gamma - 1$. Αν

$$s = 2^\gamma - 1 = 4 \cdot 2^r - 1 \leqslant 4k-1,$$

τότε η ισοτιμία (1.7.7) λύνεται πάντα αν επιλέξουμε $a_i = 1$ για $i = 1, \ldots, N$ και $a_i = 0$ για $i = N+1, \ldots, s$. Συνεπώς, $s(N) \leqslant 4k-1$ για όλους τους περιττούς N. Έτσι, ολοκληρώνεται η απόδειξη. □

Θεώρημα 1.7.10. *Υπάρχουν θετικές σταθερές $c_1 = c_1(k,s)$ και $c_2 = c_2(k,s)$ τέτοιες ώστε*

$$c_1 < \mathcal{G}(N) < c_2.$$

Επιπλέον, για αρκετά μεγάλους φυσικούς N,

$$\mathcal{G}(N, P^\nu) = \mathcal{G}(N) + O(P^{-\nu\delta_4}).$$

Απόδειξη. Ο μόνος ισχυρισμός του θεωρήματος που δεν έχουμε αποδείξει ως τώρα είναι το κάτω φράγμα για την $\mathcal{G}(N)$. Έχουμε όμως δείξει ότι υπάρχει πρώτος $p_0 = p_0(k,s)$ τέτοιος ώστε

$$\frac{1}{2} \leqslant \prod_{p>p_0} \chi_N(p) \leqslant \frac{3}{2}$$

για κάθε $N \geqslant 1$. Αφού

$$\chi_N(p) \geqslant p^{\gamma(1-s)} > 0$$

για κάθε πρώτο p και κάθε N, έπεται ότι

$$\mathcal{G}(N) = \prod_p \chi_N(p) > \frac{1}{2}\prod_{p\leqslant p_0} \chi_N(p) \geqslant \frac{1}{2}\prod_{p\leqslant p_0} p^{\gamma(1-s)} = c_1 > 0,$$

και έχουμε ολοκληρώσει την απόδειξη του θεωρήματος. □

Μπορούμε τώρα να αποδείξουμε τον ασυμπτωτικό τύπο των Hardy και Littlewood.

Θεώρημα 1.7.11 (Hardy-Littlewood)**.** *Έστω $k \geqslant 2$ και $s \geqslant 2^k + 1$. Συμβολίζουμε με $r_{k,s}(N)$ το πλήθος των αναπαραστάσεων του N ως αθροίσματος s το πλήθος k-δυνάμεων φυσικών αριθμών. Υπάρχει σταθερά $\delta = \delta(k,s) > 0$ τέτοια ώστε*

$$r_{k,s}(N) = \mathcal{G}(N)\Gamma\Big(1+\frac{1}{k}\Big)^s\Gamma\Big(\frac{s}{k}\Big)^{-1}N^{(s/k)-1} + O(N^{(s/k)-1-\delta}),$$

με την σταθερά (στο O) να εξαρτάται μόνο από τους k και s, και η $\mathcal{G}(N)$ είναι μια αριθμητική συνάρτηση τέτοια ώστε

$$c_1 < \mathcal{G}(N) < c_2$$

για κάθε N, όπου c_1 και c_2 είναι θετικές σταθερές που εξαρτώνται μόνο από τους k και s.

Απόδειξη. Θέτουμε $\delta_0 = \min\{1, \delta_1, \delta_2, \delta_3, \nu\delta_4\}$. Από τα Θεωρήματα 1.4.1 έως 1.7.10 έχουμε

$$\begin{aligned}
r_{k,s}(N) &= \int_0^1 F(\alpha)^s e(-\alpha N)\,d\alpha \\
&= \int_{\mathcal{M}} F(\alpha)^s e(-\alpha N)\,d\alpha + \int_{\Updownarrow} F(\alpha)^s e(-\alpha N)\,d\alpha \\
&= \mathcal{G}(N,P^\nu)J^*(N) + O(P^{s-k-\delta_2}) + O(P^{s-k-\delta_1}) \\
&= (\mathcal{G}(N) + O(P^{-\nu\delta_4}))(J(N) + O(P^{s-k-\delta_3})) + O(P^{s-k-\delta_2}) + O(P^{s-k-\delta_1}) \\
&= \mathcal{G}(N)J(N) + O(P^{s-k-\delta_0}) \\
&= \mathcal{G}(N)\Gamma\Big(1+\frac{1}{k}\Big)^s\Gamma\Big(\frac{s}{k}\Big)^{-1}N^{\frac{s}{k}-1} + O(N^{\frac{s-1}{k}-1}) + O(N^{\frac{s}{k}-1-\frac{\delta_0}{k}}) \\
&= \mathcal{G}(N)\Gamma\Big(1+\frac{1}{k}\Big)^s\Gamma\Big(\frac{s}{k}\Big)^{-1}N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\delta}),
\end{aligned}$$

που $\delta = \delta_0/k$. □