Προσθετική θεωρία αριθμών

Διπλωματική Εργασία

Αλέξανδρος Ηλιόπουλος

Τμήμα Μαθηματικών
Πανεπιστήμιο Αθηνών
Αθήνα – 2019

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 Προσθετική θεωρία αριθμών

Η προσθετική θεωρία αριθμών είναι ο κλάδος που μελετά αθροίσματα συνόλων ακεραίων. Αν $k \geqslant 2$ και $A_1, \ldots, A_k$ είναι σύνολα ακεραίων, το *άθροισμα συνόλων* $A_1 + \cdots + A_k$ είναι το σύνολο όλων των ακεραίων που γράφονται στη μορφή $a_1 + \cdots + a_k$, όπου $a_i \in A_i$ για $i = 1, \ldots, k$. Αν A είναι ένα σύνολο ακεραίων συμβολίζουμε με kA το άθροισμα συνόλων $A + \cdots + A$ (k φορές).

Μπορούμε επίσης να ορίσουμε αθροίσματα συνόλων σε κάθε αβελιανή ομάδα και γενικότερα σε κάθε σύνολο το οποίο είναι εφοδιασμένο με κάποια διμελή πράξη. Για παράδειγμα, μπορούμε να θεωρήσουμε αθροίσματα συνόλων στην ομάδα $\mathbb{Z}/m\mathbb{Z}$ των κλάσεων ισοτιμίας $\bmod m$ ή στην ομάδα $\mathbb{Z}^n$ των ακεραίων σημείων του $\mathbb{R}^n$.

Αρχετυπικό θεώρημα του κλάδου της προσθετικής θεωρίας αριθμών είναι το κλασικό θεώρημα του Lagrange. Το 1621 ο Bachet διατύπωσε την εικασία ότι κάθε φυσικός αριθμός n μπορεί να γραφτεί ως το άθροισμα το πολύ τεσσάρων τέλειων τετραγώνων. Ο Euler προσπάθησε ανεπιτυχώς να επιλύσει το πρόβλημα. Ωστόσο κατάφερε, βασιζόμενος στην ταυτότητα των τεσσάρων τετραγώνων που ανακάλυψε το 1748, να δείξει ότι το πρόβλημα μπορεί να αναχθεί στην περίπτωση που ο n είναι πρώτος. Το 1770 ο Lagrange χρησιμοποιώντας την παρατήρηση του Euler κατάφερε να αποδείξει το λεγόμενο «θεώρημα των τεσσάρων τετραγώνων».

Θεώρημα 1.1.1 (Lagrange)**.** *Κάθε μη αρνητικός ακέραιος είναι το άθροισμα 4 τέλειων τετραγώνων.*

Απόδειξη. Είναι εύκολο να ελέγξουμε ότι ισχύει η πολυωνυμική ταυτότητα

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

όπου

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$
$$z_2 = x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3$$
$$z_3 = x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2$$
$$z_4 = x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2$$

Είναι φανερό λοιπόν ότι αν δύο αριθμοί γράφονται ως άθροισμα τεσσάρων τέλειων τετραγώνων, τότε και το γινόμενο τους είναι επίσης άθροισμα τεσσάρων τέλειων τετραγώνων. Καθώς κάθε αριθμός είναι γινόμενο πρώτων αριθμών, αρκει να δείξουμε το ζητούμενο για κάθε πρώτο αριθμό. Επίσης $2 = 1^2 + 1^2 + 0^2 + 0^2$ και συνεπώς θεωρούμε μόνο περιττούς πρώτους p.

Το σύνολο των τετραγώνων

$$\{a^2 : a = 0, 1, \ldots, (p-1)/2\}$$

αντιπροσωπέυει $(p+1)/2$ διαφορετκές κλάσεις υπολοίπων modulo p. Ομοίως, το σύνολο των ακεραίων

$$\{-b^2 - 1 : b = 0, 1, \ldots, (p-1)/2\}$$

αντιπροσωπέυει $(p+1)/2$ διαφορετκές κλάσεις υπολοίπων modulo p. Καθώς υπάρχουν μόνο p διαφορετκές κλάσεις υπολοίπων modulo p, από την Αρχή του Περιστερώνα πρέπει να υπάρχουν ακέραιοι a και b τέτοιοι ώστε $0 \leqslant a, b \leqslant (p-1)/2$ και

$$a^2 \equiv -b^2 - 1 \bmod p,$$

ή ισοδύναμα

$$a^2 + b^2 + 1 \equiv 0 \bmod p.$$

Έστω $a^2 + b^2 + 1 = np$. Τότε,

$$p \leqslant np = a^2 + b^2 + 1^2 + 0^2 \leqslant 2\left(\frac{p-1}{2}\right)^2 + 1 < \frac{p^2}{2} + 1 < p^2,$$

και έτσι

$$1 \leqslant n < p.$$

Έστω m ο ελάχιστος θετικός ακέραιος τέτοιος ώστε ο mp να είναι το άθροισμα τεσσάρων τέλειων τετραγώνων. Συνεπώς υπάρχουν ακέραιοι x_1, x_2, x_3, x_4 τέτοιοι ώστε

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

και

$$1 \leqslant m \leqslant n < p.$$

Πρέπει να δείξουμε ότι $m = 1$.

Ας υποθέσουμε ότι $m \neq 1$. Τότε $1 < m < p$. Επιλέγουμε ακέραιους y_i ώστε

$$y_i \equiv x_i \bmod m$$

και

$$\frac{-m}{2} < y_i < \frac{m}{2}$$

για $i = 1, \ldots, 4$. Έτσι

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \bmod m$$

και

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

για κάποιον μη αρνητικό ακέραιο r. Αν $r = 0$, έχουμε $y_i = 0$ για κάθε i και κάθε x_i διαιρείται από τον m^2. Προκύπτει δηλαδή ότι ο mp διαιρείται από τον m^2, και συνεπώς ο p διαιρείται από τον m. Αυτό είναι όμως αδύνατο, καθώς ο p είναι πρώτος και $1 < m < p$. Άρα, $r \geqslant 1$ και

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2 \geqslant 4(m/2)^2 = m^2$$

Επίσης, $r = m$ αν και μονο αν ο m είναι άρτιος και $y_i = m/2$ για κάθε i. Σε αυτήν την περίπτωση, $x_i = m/2 \bmod m$ για κάθε i, και έτσι $x_i^2 \equiv (m/2)^2 \bmod m^2$ και

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 4(m/2)^2 = m \equiv 0 \bmod m^2.$$

Από αυτό προκύπτει ότι ο p διαιρείται από τον m, το οποίο είναι αντίφαση. Συνεπώς,

$$1 \leqslant r < p < m.$$

Εφαρμόζοντας τώρα την αρχική πολυωνυμική ταυτότητα παίρνουμε

$$m^2rp = (mp)(mr) = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

όπου τα z_i προσδιορίζονται από τις σχέσεις. Καθώς $x_i \equiv y_i \bmod m$, από τις σχέσεις αυτές συμπεραίνουμε ότι $z_i \equiv 0 \bmod m$ για $i = 1, \ldots, 4$. Έστω $w_i = z_i/m$. Τότε οι $w_1, \ldots, w_4$ είναι ακέραιοι και

$$rp = w_1^2 + w_2^2 + w_3^2 + w_4^2,$$

το οποίο αντίκειται στην ελαχιστικότητα του m. Άρα $m = 1$ και ο πρώτος p είναι το άθροισμα τεσσάρων τέλειων τετραγώνων. Αυτό ολοκληρώνει και την απόδειξη του θεωρήματος. □

1.2 Το πρόβλημα του Waring

Το πρώτο μέρος της παρούσας εργασίας είναι αφιερωμένο στο Πρόβλημα του Waring. Αμέσως μετά από την απόδειξη του θεωρήματος του Lagrange, ο Waring διατύπωσε χωρίς απόδειξη στο βιβλίο του Meditationes Algebraicae την υπόθεση ότι κάθε φυσικός μπορεί να γραφτεί ως το άθροισμα το πολύ 9 κύβων, ως άθροισμα το πολύ 16 τετάρτων δυνάμεων και ούτω καθεξής. Η εικασία αυτή έγινε γνωστή ως το Πρόβλημα του Waring. Η ακριβής διατύπωση του προβλήματος είναι η ακόλουθη:

Πρόβλημα του Waring: Για κάθε φυσικό αριθμό k, υπάρχει ένας αριθμός s, ο οποίος εξαρτάται μόνο από τον k, τέτοιος ώστε κάθε φυσικός αριθμός μπορεί να γραφτεί ως άθροισμα το πολύ s k-οστών δυνάμεων θετικών ακεραίων.

Ο ελάχιστος τέτοιος αριθμός s, συμβολίζεται με $g(k)$.

Παρουσιάζουμε τις τρεις μεθόδους με τις οποίες έχει επιλυθεί το πρόβλημα του Waring. Η παρουσίαση γίνεται με χρονολογική σειρά. Παρακάτω δίνουμε μια συνοπτική περιγραφή του περιεχομένου του μέρους αυτού.

Κεφάλαιο 2. Η πρώτη απόδειξη του προβλήματος του Waring δόθηκε το 1909 από τον David Hilbert ο οποίος το απέδειξε χρησιμοποιώντας ένα δύσκολο συνδυαστικό επιχείρημα βασισμένο σε αλγεβρικές ταυτότητες. Σε αυτό το κεφάλαιο παρουσιάζουμε μια εκδοχή της αρχικής απόδειξης του Hilbert η οποία οφείλεται στους Hausdorff και Stridsberg.

Το 1859 ο Liouville χρησιμοποιώντας την ταυτότητα

$$(x_1^2+x_2^2+x_3^2+x_4^2)^2 = \frac{1}{6}\sum_{1\leqslant i<j\leqslant 4}(x_i+x_j)^4 + \frac{1}{6}\sum_{1\leqslant i<j\leqslant 4}(x_i-x_j)^4$$

σε συνδυασμό με το θεώρημα του Lagrange, κατάφερε με πολύ απλά επιχειρήματα να δείξει ότι $g(4)\leqslant 53$.

Για κάθε $n\geqslant 0$ ορίζουμε το *πολυώνυμο Hermite* $H_n(x)$ ως εξής:

$$H_n(x) = \Big(-\frac{1}{2}\Big)^n e^{x^2}\frac{d^n}{dx^n}(e^{-x^2}).$$

Με την βοήθεια αυτών των πολυωνύμων καταφέρνουμε να αποδείξουμε μια γενίκευση της παρατήρησης του Liouville. Συγκεκριμένα αποδεικνύουμε την ακόλουθη ταυτότητα:

Θεώρημα 1.2.1 (ταυτότητα του Hilbert)**.** *Για κάθε $k\geqslant 1$ και $r\geqslant 1$ μπορούμε να βρούμε ακέραιο M και θετικούς ρητούς αριθμούς a_i και ακεραίους $b_{i,j}$, για $i=1,\dots,M$ και $j=1,\dots,r$, τέτοιους ώστε*

$$(x_1^2+\cdots+x_r^2)^k = \sum_{i=1}^{M} a_i(b_{i,1}x_1+\cdots+b_{i,r}x_r)^{2k}$$

για κάθε r-άδα μη αρνητικών ακεραίων $x_1,\dots,x_r$.

Από το παραπάνω θεώρημα και το θεώρημα του Lagrange παίρνουμε την ακόλουθη πρόταση η οποία αποτελεί ουσιαστικό βήμα για την απόδειξη του θεωρήματος του Hilbert.

Θεώρημα 1.2.2. *Αν το πρόβλημα του Waring έχει καταφατική απάντηση για τον εκθέτη k τότε έχει καταφατική απάντηση και για τον εκθέτη $2k$.*

Επίσης η ταυτότητα του Hilbert θα μας δώσει το ακόλουθο σημαντικό αποτέλεσμα:

Λήμμα 1.2.3. *Έστω $k\geqslant 2$ και $0\leqslant \ell\leqslant k$. Υπάρχουν θετικοί ακέραιοι $B_{0,\ell},B_{1,\ell},\dots,B_{\ell-1,\ell},M_\ell$ και θετικοί ρητοί $a_1,\dots,a_{M_\ell}$ που εξαρτώνται μόνο από τους k και ℓ, τέτοιοι ώστε η*

$$x^{2\ell}T^{k-\ell}+\sum_{i=0}^{\ell-1}B_{i,\ell}x^{2i}T^{k-i} = \sum_{i=1}^{M_\ell}a_i x_i^k,$$

να έχει λύση στους μη αρνητικούς ακεραίους $x_1,\dots,x_{M_\ell}$ για όλους τους ακεραίους x και T που ικανοποιούν την

$$x^2\leqslant T.$$

Οι δύο παραπάνω προτάσεις θα οδηγήσουν και στο κεντρικό αποτέλεσμα αυτής της παραγράφου, το θεώρημα του Hilbert, δηλαδή την απόδειξη του προβλήματος του Waring.

Η απόδειξη αυτή του Hilbert, υστερεί στο ότι δεν μας δίνει άμεση εκτίμηση για κάποιο άνω φράγμα της ποσότητας $g(k)$. Πρώτος ο 1953 ο Rieger από την μέθοδο αυτή πέτυχε το άνω φράγμα

$$g(k) \leqslant (2k+1)^{260(k+3)^{3k+8}}.$$

Ο Pollack το 2011 έδειξε ότι για κάθε $k \geqslant 2$ μπορούμε να πετύχουμε το άνω φράγμα

$$g(k) < (2k+1)^{1808k^5},$$

που είναι αρκετά αδύναμο.

Κεφάλαιο 3. Σε αυτό το κεφάλαιο αναπτύσσουμε ορισμένα αναλυτικά εργαλεία τα οποία θα μας βοηθήσουν στην επίλυση του προβλήματος του Waring με την λεγόμενη κυκλική μέθοδο των Hardy-Littlewood. Αυτά είναι η ανισότητα του Weyl και το λήμμα του Hua.

Μας ενδιαφέρει να εκτιμήσουμε το μέτρο αθροισμάτων της μορφής

$$S(f) = \sum_{n=N_1+1}^{N_2} e(f(n)),$$

όπου $f(n) = \alpha x^k + \cdots$ είναι ένα πολυώνυμο βαθμού k και με $e(\alpha)$ συμβολίζουμε τον μιγαδικό αριθμό $e^{2\pi i\alpha}$.

Για $k = 1$ προκύπτει άμεσα η ανισότητα

$$\left| \sum_{n=N_1+1}^{N_2} e(\alpha n) \right| \leqslant \min\{N_2 - N_1, \|\alpha\|^{-1}\}$$

όπου με $\|\alpha\|$ συμβολίζουμε την απόσταση του πραγματικού αριθμου α από το $\mathbb{Z}$ που ορίζεται από την

$$\|\alpha\| = \min\{|n-\alpha| : n \in \mathbb{Z}\} = \min\{\{\alpha\}, 1-\{\alpha\}\}.$$

Θα εισάγουμε την έννοια του *τελεστή διαφορών προς τα εμπρός* Δ_d που είναι γραμμικός τελεστής ο οποίος ορίζεται για μια συνάρτηση f από τον τύπο

$$\Delta_d(f)(x) = f(x+d) - f(x).$$

Ο Weyl παρατήρησε ότι μπορούμε να γράψουμε το $|S(f)|^2$ ως εξής:

$$|S(f)|^2 = \sum_{n=N_1+1}^{N_2} \sum_{m=N_1+1}^{N_2} e\big(f(m) - f(n)\big),$$

όπου θέτοντας $m = n + d$ μπορούμε να πετύχουμε την

$$|S(f)|^2 = \sum_{|d|<N} S_d(f),$$

όπου $N = N_2 - N_1$ και

$$S_d(f) = \sum_{n \in I(d)} e(\Delta_d(f)(n))$$

και $I(d)$ είναι διάστημα διαδοχικών ακεραίων που περιέχεται στο $[N_1 + 1, N_2]$.

Αυτή η απλή αλλά πολύ σημαντική παρατήρηση παίζει σημαντικό ρόλο στην εκτίμηση του μέτρου του $S(f)$ καθώς μας δίνει τη δυνατότητα να χρησιμοποιήσουμε επιχειρήματα επαγωγής στο βαθμό του πολυωνύμου $f(n)$, μιας και ο βαθμός του $\Delta_d(f)(n)$ είναι κατά ένα μικρότερος.

Όπως θα δούμε, το μέτρο του $S(f)$ εξαρτάται από την ρητή προσέγγιση του μεγιστοβάθμιου συντελεστή α και πιο συγκεκριμένα από τον παρονομαστή της προσέγγισης αυτής. Με τον όρο *ρητή προσέγγιση* εννοούμε την ύπαρξη ενός ζεύγους ακεραίων $q \geqslant 1$ και a με $(a, q) = 1$ και

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}.$$

Η ύπαρξη μιας τέτοιας προσέγγισης εξασφαλίζεται από ένα γνωστό συνδυαστικό θεώρημα του Dirichlet.

Αναφέρουμε τα δύο βασικά αποτελέσματα του κεφαλαίου αυτού:

Θεώρημα 1.2.4 (ανισότητα του Weyl)**.** *Έστω $f(x) = \alpha x^k + \cdots$ πολυώνυμο βαθμού $k \geqslant 2$ με πραγματικούς συντελεστές. Υποθέτουμε ότι ο α έχει ρητή προσέγγιση a/q τέτοια ώστε*

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q^2},$$

όπου $q \geqslant 1$ και $(a, q) = 1$. Έστω

$$S(f) = \sum_{n=1}^{N} e(f(n)).$$

Έστω $K = 2^{k-1}$ και $\varepsilon > 0$. Τότε,

$$S(f) \ll N^{1+\varepsilon}\Big(\frac{1}{N} + \frac{1}{q} + \frac{q}{N^k}\Big)^{1/K},$$

με την σταθερά να εξαρτάται μόνο από τους k και ε.

Θεώρημα 1.2.5 (λήμμα του Hua)**.** *Για $k \geqslant 2$ ορίζουμε*

$$T(\alpha) = \sum_{n=1}^{N} e(\alpha n^k).$$

Τότε, για κάθε $\varepsilon > 0$ ισχύει

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

με την σταθερά να εξαρτάται μόνο από τους k και ε.

Κεφάλαιο 4. Το 1920, 10 χρόνια μετά την απόδειξη του Hilbert, οι Hardy και Littlewood κατάφεραν να αποδείξουν με αναλυτικές μεθόδους το πρόβλημα του Waring. Αντικείμενο αυτού του κεφαλαίου είναι η παρουσίαση αυτής της μεθόδου.

Η ιδέα της μεθόδου προέρχεται από την προγενέστερη μελέτη από τους Hardy και Ramanujan της συνάρτησης διαμερισεων $p(n)$ και 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 $\varrho \in (0,1)$. Από αυτή τη σχέση προέρχεται και το όνομα «κυκλική μέθοδος».

Στην παρουσίασή μας θα υιοθετήσουμε την προσέγγιση του Vinogradov ο οποίος μετέπειτα βελτίωσε σημαντικά τη μέθοδο αυτή.

Ορίζουμε $r_{k,s}(N)$ να είναι πλήθος των αναπαραστάσεων του N ως αθροίσματος s θετικών k-οστών δυνάμεων. 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

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

Θέτουμε

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

Αντί για την δυναμοσειρά χρησιμοποιούμε το τριγωνομετρικό πολυώνυμο

$$F(\alpha) = \sum_{n=1}^{P} e(\alpha n^k),$$

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

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

Βλέπουμε λοιπόν ότι το πρόβλημα με αυτόν τον τρόπο ανάγεται στον υπολογισμό του ολοκληρώματος αυτού. Για να υπολογίσουμε το ολοκλήρωμα αυτό χωρίζουμε το διάστημα $[0,1]$ σε δύο ξένα μεταξύ τους σύνολα, τα *μείζονα τόξα* $\mathfrak{M}$ και τα *ελλάσσονα τόξα* $\mathfrak{m} = [0,1] \setminus \mathcal{M}$. Τα μείζονα τόξα αποτελούνται στην ουσία από όλους τους πραγματικούς εντός του διαστήματος $[0,1]$ οι οποίοι έχουν, κατά κάποιο τρόπο, «καλή» ρητή προσέγγιση.

Χρησιμοποιώντας την ανισότητα Weyl και το λήμμα του Hua μπορούμε να δείξουμε ότι παρόλο που στα ελάσσονα τόξα βρίσκεται το μεγαλύτερο μέρος του μοναδιαίου διαστήματος, το ολοκλήρωμα πάνω σε αυτά είναι «αμελητέο». Συγκεκριμένα θα δείξουμε ότι για $k \geqslant 2$ και $s \geqslant 2^k + 1$ υπάρχει $\delta_1 > 0$ τέτοιος ώστε

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

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

Για να υπολογίσουμε το ολοκλήρωμα στα μείζονα τόξα θα ορίσουμε 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 αποδείξουμε ότι μπορούμε να εκφράσουμε το ολοκλήρωμα στα μείζονα τόξα ως γινόμενο δύο όρων, του *ιδιάζοντος ολοκληρώματος*

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

και της *ιδιάζουσας σειράς*

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

συν ένα παράγοντα σφάλματος. Συγκεκριμένα θα δείξουμε ότι υπάρχει $\delta_2 > 0$ τέτοιος ώστε

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

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

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

όπου $\Gamma(x)$ είναι η συνάρτηση Γάμμα. Επίσης, συγκεκριμένες αριθμοθεωρητικές ιδιότητες της σειράς $\mathfrak{G}(N)$ θα μας επιτρέψουν να δείξουμε ότι $\mathfrak{G}(N) > 0$ για κάθε N και ότι υπάρχουν σταθερές $c_1 > 0$ και $c_2 > 0$ που εξαρτώνται μόνο από τους k και s, τέτοιες ώστε

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

για όλους τους φυσικούς N. Έτσι θα καταλήξουμε στον περίφημο ασυμπτωτικό τύπο των Hardy και Littlewood:

Θεώρημα 1.2.6 (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*

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

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

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

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

Η δύναμη της μεθόδου των Hardy και Littlewood φαίνεται αμέσως από το γεγονός ότι δίνει το άνω φράγμα

$$g(k) \leqslant 2^k + 1$$

το οποίο είναι πολύ ισχυρότερο από τα άνω φράγματα που μπορεί να πετύχει κανείς με τη μέθοδο του Hilbert. Η κυκλική μέθοδος έκανε δυνατό τον προσδιορισμό του $g(k)$ για τις περισσότερες τιμές του φυσικού αριθμού k. Ενδεικτικά ο Mahler απέδειξετο 1957 ότι

$$g(k) = 2^k + \Big[\Big(\frac{3}{2}^k\Big)\Big] - 2,$$

για όλες εκτός από το πολύ πεπερασμένες το πλήθος τιμές του αριθμού k.

Η έρευνα στράφηκε επιπλέον και στη μελέτη του αριθμού $G(k)$, δηλαδή του ελάχιστου αριθμού που είναι τέτοιος ώστε κάθε αρκετά μεγάλος αριθμός να μπορεί να εκφραστει ως άθροισμα το πολύ $G(k)$ το πλήθος k-οστών δυνάμεων φυσικών. Ο Vinogradov απέδειξε χρησιμοποιώντας την τεχνική αυτή ότι

$$G(k) \leqslant 3k(\log k + 11)$$

και τελικά το 1959 ότι

$$G(k) \leqslant k(2\log k + 2\log\log k + C\log\log\log k).$$

Περαιτέρω βελτιώσεις έχουν επιτευχθεί από τους Vaughan, Wooley, Karatsuba και άλλους.

Εκτός από το ίδιο το πρόβλημα του Waring, η κυκλική μέθοδος αποτέλεσε και αποτελεί εργαλείο αντιμετώπισης πολλών προβλημάτων προσθετικής φύσεως. Χαρακτηριστικό παράδειγμα αποτελεί η χρήση της μεθόδου για την αντιμετώπιση ενός ακόμα γνωστού προβλήματος της προσθετικής θεωρίας αριθμών, της εικασίας του Goldbach. Το 1957 ο Vinogradov κατάφερε να δείξει ότι κάθε αρκετά μεγάλος περιττός αριθμός μπορεί να γραφτεί ως άθροισμα 3 πρώτων.

Κεφάλαιο 5. Σε αυτό το κεφάλαιο παρουσιάζουμε μια στοιχειώδη απόδειξη για το πρόβλημα του Waring που δόθηκε το 1942 από τον Linnik, ο οποίος βασίστηκε στις ιδέες του Schnirelmann.

Έστω A ένα σύνολο μη αρνητικών ακεραίων το οποίο περιέχει το 0. Με $A^{(s)}$ συμβολίζουμε το σύνολο όλων των αριθμών οι οποίοι μπορούν να εκφραστούν ως άθροισμα s το πλήθος στοιχείων του συνόλου A. Λέμε ότι το σύνολο A είναι *προσθετική βάση του* $\mathbb{N}$ αν υπάρχει φυσικός αριθμός s τέτοιος ώστε $A^{(s)} = \mathbb{N}$. Με την έννοια αυτή, το πρόβλημα του Waring μπορεί να αναδιατυπωθεί ως εξής:

Πρόβλημα του Waring: Για κάθε $k \in \mathbb{N}$, το σύνολο $A = \{0^k, 1^k, 2^k, \dots\}$ είναι προσθετική βάση του $\mathbb{N}$.

Για ένα σύνολο A όπως παραπάνω θεωρούμε την αριθμητική συνάρτηση $A(n)$ που μετρά το πλήθος των όρων του συνόλου A που δεν ξεπερνούν έναν δεδομένο φυσικό n, δίχως να προσμετρήσουμε τον αριθμό 0 και ορίζουμε την *πυκνότητα κατά Schnirelmann* του A με

$$\sigma(A) = \inf_n \frac{A(n)}{n}.$$

Τα παραπάνω σύνολα, θεωρώντας τα σε αύξουσα σειρά θα τα λέμε για ευκολία *ακολουθίες*.

Στην πρώτη παράγραφο αυτού του κεφαλαίου αποδεικνύουμε τα δύο αποτελέσματα του Schnirelmann:

Θεώρημα 1.2.7 (Schnirelmann)**.** *Έστω A, B ακολουθίες φυσικών αριθμών. Τότε*

$$\sigma(A + B) \geqslant \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

Χρησιμοποιώντας αυτήν την ανισότητα θα αποδείξουμε το επόμενο θεώρημα:

Θεώρημα 1.2.8 (Schnirelmann)**.** *Κάθε ακολουθία θετικής πυκνότητας κατά Schnirelmann είναι προσθετική βάση των φυσικών αριθμών.*

Ο Linnik κατάφερε να επιλύσει το Πρόβλημα του Waring δείχνοντας ότι υπάρχει κάποιος φυσικός s τέτοιος ώστε το σύνολο $A_k^{(s)}$, όπου $A_k = \{0^k, 1^k, 2^k, \dots\}$, να έχει θετική πυκνότητα κατά Schnirelmann. Για να το πετύχει αυτό απέδειξε μια σειρά από λήμματα που αφορούν το πλήθος των λύσεων γραμμικών εξισώσεων και τα οποία παρουσιάζουμε στην δεύτερη παράγραφο αυτού του κεφαλαίου.

Στην τρίτη και τελευταία παράγραφο χρησιμοποιώντας τα αποτελέσματα που έχουμε στα χέρια μας αποδεικνύουμε το λεγόμενο «κύριο λήμμα» από το οποίο το συμπέρασμα μας έπεται άμεσα και του οποίου η ακριβής διατύπωση είναι η εξής:

Λήμμα 1.2.9 (κύριο λήμμα)**.** *Υπάρχει $s = s(k)$ τέτοιος ώστε, για κάθε $N \geqslant 1$, να ισχύει*

$$r_{k,s}(m) \leqslant cN^{\frac{s}{k}-1},$$

για $1 \leqslant m \leqslant N$, όπου η σταθερά c εξαρτάται μόνο από το k.

1.3 Το θεώρημα του Freiman

Με τον όρο «ευθύ πρόβλημα» στην προσθετική θεωρία αριθμών εννοούμε ένα ερώτημα το οποίο αφορά τη δομή και τις ιδιότητες του αθροίσματος συνόλων kA για δοθέν σύνολο A. Για παράδειγμα,

το θεώρημα του Lagrange είναι ένα «ευθύ αποτέλεσμα» υπό την έννοια ότι, για το σύνολο $\mathbb{Z}_+^{(2)}$ των μη αρνητικών τέλειων τετραγώνων, εξασφαλίζει ότι

$$\mathbb{Z}_+ = 4\mathbb{Z}_+^{(2)}.$$

Το διάσημο θεώρημα του Vinogradov, ότι κάθε αρκετά μεγάλος περιττός φυσικός γράφεται ως άθροισμα τριών πρώτων, μπορεί να διατυπωθεί ως εξής: αν $2 \cdot \mathbb{Z}_+ + 1$ είναι το σύνολο των περιττών πρώτων και $\mathbb{P}$ είναι το σύνολο των πρώτων αριθμών, τότε το

$$(2 \cdot \mathbb{Z}_+ + 1) \setminus 3\mathbb{P}$$

είναι πεπερασμένο. Η «εικασία του Goldbach», η οποία παραμένει ανοικτό πρόβλημα, ισχυρίζεται ότι το σύνολο $2\mathbb{P}$ περιέχει όλους τους άρτιους φυσικούς που είναι μεγαλύτεροι από 2.

Στο δεύτερο μέρος της παρούσας εργασίας ασχολούμαστε με την ανάλυση των αθροισμάτων της μορφής $A_1 + \cdots + A_k$ για γενικότερα σύνολα A_i. Θα θεωρήσουμε πεπερασμένα, και όχι άπειρα, υποσύνολα μιας προσθετικής ομάδας G. Ένα από τα βασικά προβλήματα του κλάδου είναι το «αντίστροφο πρόβλημα», το οποίο ρωτάει, για παράδειγμα, τι μπορούμε να πούμε για την δομή δύο υποσυνόλων A και B της G αν γνωρίζουμε ότι ο πληθάριθμος του $A + B$ είναι μικρός. Το θεώρημα του Freiman ισχυρίζεται ότι αν A είναι ένα πεπερασμένο σύνολο ακεραίων τέτοιο ώστε το $2A$ να έχει μικρό πληθάριθμο, τότε το A είναι μεγάλο υποσύνολο μιας πολυδιάστατης αριθμητικής προόδου. Η ακριβής διατύπωση αυτού του αντίστροφου θεωρήματος είναι η εξής.

Θεώρημα 1.3.1 (Freiman). *Έστω A ένα πεπερασμένο σύνολο ακεραίων τέτοιο ώστε $|2A| \leqslant c|A|$. Υπάρχουν ακέραιοι a και $q_1, \dots, q_n, \ell_1, \dots, \ell_n$ τέτοιοι ώστε*

$$A \subseteq Q = \{a + x_1 q_1 + \cdots + x_n q_n : 0 \leqslant x_i < \ell_i \ \text{ για κάθε } i = 1, \dots, n\},$$

όπου $|Q| \leqslant c'|A|$ και οι n και c' εξαρτώνται μόνο από τη σταθερά c.

Η απόδειξη αυτού του θεωρήματος χρησιμοποιεί βαθιά αποτελέσματα από την γεωμετρία των αριθμών και την θεωρία γραφημάτων. Παρουσιάζουμε μια μεταγενέστερη απόδειξη ενός γενικότερου αποτελέσματος που οφείλεται στον Ruzsa, καθώς και τα εργαλεία που απαιτούνται για την απόδειξη.

Κεφάλαιο 6. Σε αυτό το εισαγωγικό κεφάλαιο παρουσιάζουμε πιο στοιχειώδεις εκτιμήσεις για αθροίσματα συνόλων και εισάγουμε κάποιες βασικές έννοιες της περιοχής για μια πρώτη εξοικείωση του αναγνώστη με το θέμα. Μερικά από τα αποτελέσματα μπορούν να ιδωθούν ως απλούστερα υποκατάστατα του θεωρήματος του Freiman ενώ κάποια άλλα θα χρειαστούν στην απόδειξη του θεωρήματος του Freiman. Η πρώτη έννοια που συζητάμε είναι αυτή της *σταθεράς διπλασιασμού*, που ορίζεται από την

$$\sigma(A) = \frac{|A + A|}{|A|},$$

όπου $|A|$ είναι ο πληθάριθμος ενός πεπερασμένου συνόλου A. Η σταθερά διπλασιασμού ενός συνόλου είναι πάντα τουλάχιστον ίση με 1, μπορεί όμως να είναι πολύ μεγαλύτερη. Αν A είναι το σύνολο των όρων μιας γεωμετρικής προόδου, για παράδειγμα αν $A = \{1, 2, 2^2, \dots, 2^{N-1}\}$, τότε $\sigma(A) = (N+1)/2$. Στο αντίθετο άκρο, αν A είναι το σύνολο των όρων μιας αριθμητικής προόδου μήκους N τότε μπορεί κανείς να ελέγξει ότι $\sigma(A) = 2 - \frac{1}{N}$. Το τελευταίο παράδειγμα δείχνει ότι

μικρή σταθερά διπλασιασμού σχετίζεται με την δομή της αριθμητικής προόδου, και το θεώρημα του Freiman επιβεβαιώνει αυτήν την διασύνδεση.

Ένα πρώτο αποτέλεσμα αυτού του κεφαλαίου είναι η ανισότητα του Ruzsa, η οποία μας επιτρέπει να ορίσουμε μια «μετρική» στον χώρο των προσθετικών συνόλων και μετράει πόσο μικρά είναι τα αθροίσματα τους: αν A και B είναι πεπερασμένα υποσύνολα μιας αβελιανής ομάδας G, η απόσταση Ruzsa των A και B είναι η ποσότητα

$$d(A,B) = \log \frac{|A-B|}{\sqrt{|A|\,|B|}}.$$

Συνέπεια της ανισότητας του Ruzsa είναι το γεγονός ότι η d ικανοποιεί την τριγωνική ανισότητα.

Μια άλλη βασική έννοια είναι αυτή της *προσθετικής ενέργειας*. Αν A και B είναι πεπερασμένα υποσύνολα της αβελιανής ομάδας G τότε η προσθετική ενέργεια των A και B είναι η ποσότητα

$$E(A,B) = |\{(a,a_1,b,b_1) \in A\times A\times B\times B : a+b = a_1+b_1\}|.$$

Συζητάμε διάφορες ανισότητες που συνδέουν την προσθετική ενέργεια $E(A,B)$ με τον πληθάριθμο των $|A+B|$ και $|A-B|$. Μια συνέπεια αυτών των ανισοτήτων είναι η δεύτερη ανισότητα του Ruzsa, η οποία ισχυρίζεται ότι

$$d(A,-B) \leqslant 3d(A,B).$$

Οι ανισότητες του Ruzsa μας επιτρέπουν να ελέγχουμε την απόσταση δύο συνόλων $A,B\subseteq G$. Χαρακτηριστικό αποτέλεσμα που προκύπτει μέσω αυτού του «λογισμού του Ruzsa» είναι η *ανισότητα πολλαπλού αθροίσματος*, η οποία ισχυρίζεται ότι αν A είναι ένα πεπερασμένο υποσύνολο της αβελιανής ομάδας G με $\sigma(A)\leqslant c$ και αν $k,l\in\mathbb{Z}_+$ με $(k,l)\neq(0,0)$, τότε υπάρχει σταθερά $\gamma(k,l)$ ώστε

$$|kA-lA| \ll K^{\gamma(k,l)}|A|.$$

Στο Κεφάλαιο 7 θα δείξουμε μια ακριβέστερη μορφή αυτού του αποτελέσματος, η οποία θα χρησιμοποιηθεί στην απόδειξη του θεωρήματος του Freiman.

Τέλος, σε αυτό το κεφάλαιο αποδεικνύουμε κάποια *λήμματα κάλυψης* τα οποία δίνουν συνθήκες που εξασφαλίζουν ότι κάποιο σύνολο A καλύπτεται οικονομικά από μεταφορές κάποιου άλλου συνόλου B.

Κεφάλαιο 7. Σε αυτό το κεφάλαιο παρουσιάζουμε τα αποτελέσματα της Γεωμετρίας των Αριθμών που θα χρειαστούμε για την απόδειξη του θεωρήματος του Freiman. Ένα υποσύνολο Λ του $\mathbb{R}^n$, $n\geqslant 2$, λέγεται *πλέγμα* αν υπάρχουν γραμμικά ανεξάρτητα διανύσματα $u_1,\dots,u_n\in\mathbb{R}^n$ ώστε

$$\Lambda = \{x\in\mathbb{R}^n : x = m_1u_1+\cdots+m_nu_n, m_i\in\mathbb{Z}\}.$$

Τότε λέμε ότι το $\{u_1,\dots,u_n\}$ είναι μια *βάση* του πλέγματος Λ. Αν Λ είναι ένα πλέγμα στον $\mathbb{R}^n$ και $u_1,\dots,u_n$ μια βάση του, τότε το παραλληλεπίπεδο

$$Q = \Big\{\sum_{i=1}^n a_iu_i : 0\leqslant a_i<1\Big\}$$

λέγεται θεμελιώδες παραλληλεπίπεδο του πλέγματος. Ο όγκος $|Q|$ του Q λέγεται *ορίζουσα του πλέγματος* και συμβολίζεται με $\det\Lambda$. Αποδεικνύουμε ότι ο όγκος του θεμελιώδους παραλληλεπιπέδου είναι ανεξάρτητος από την επιλογή της βάσης.

Στη συνέχεια παρουσιάζουμε τα δύο θεμελιώδη θεωρήματα του Minkowski. Το πρώτο θεώρημα του Minkowski εξασφαλίζει την ύπαρξη μη μηδενικού σημείου με ακέραιες συντεταγμένες σε κάθε ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$ που έχει όγκο μεγαλύτερο από 2^n.

Θεώρημα 1.3.2. *Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Αν $|K| > 2^n$, τότε το K περιέχει τουλάχιστον ένα $u \in \mathbb{Z}^n \setminus \{0\}$.*

Για το δεύτερο θεώρημα, εισάγουμε πρώτα τα διαδοχικά ελάχιστα ενός κυρτού σώματος ως προς το πλέγμα $\mathbb{Z}^n$. Για δοθέν συμμετρικό κυρτό σώμα K στον $\mathbb{R}^n$ και για κάθε $i = 1, \dots, n$ ορίζουμε

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^n) \geqslant i\},$$

όπου $\dim(\lambda K \cap \mathbb{Z}^n)$ είναι η διάσταση του υποχώρου που παράγεται από τα ακέραια σημεία του λK. Οι αριθμοί λ_i ονομάζονται *διαδοχικά ελάχιστα* του K (ως προς το πλέγμα $\mathbb{Z}^n$). Είναι φανερό ότι $0 < \lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_n$.

Θεώρημα 1.3.3 (δεύτερο θεώρημα του Minkowski)**.** *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε,*

$$\lambda_1 \lambda_2 \cdots \lambda_n |K| \leqslant 2^n.$$

Άμεση γενίκευση του θεωρήματος για τυχόν πλέγμα Λ στον $\mathbb{R}^n$ είναι η εξής: Έστω Λ πλέγμα στον $\mathbb{R}^n$, και K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε,

$$\lambda_1 \lambda_2 \cdots \lambda_n |K| \leqslant 2^n \det \Lambda,$$

όπου

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda K \cap \Lambda) \geqslant i\}, \quad i = 1, \dots, n.$$

Η εφαρμογή των παραπάνω που μας ενδιαφέρει είναι το επόμενο θεώρημα, το οποίο θα χρησιμοποιηθεί στην απόδειξη του θεωρήματος του Freiman. Έστω $m \geqslant 2$ και έστω $u = (u_1, \dots, u_n)$ και $v = (v_1, \dots, v_n) \in \mathbb{Z}^n$. Γράφουμε $u \equiv v \bmod m$ αν $u_i \equiv v_i \bmod m$ για κάθε $i = 1, \dots, n$.

Θεώρημα 1.3.4. *Έστω $m \geqslant 2$ και $r_1, \dots, r_n$ ακέραιοι τέτοιοι ώστε ο μέγιστος κοινός διαιρέτης των $r_1, \dots, r_n, m$ να είναι ίσος με 1. Θέτουμε $r = (r_1, \dots, r_n) \in \mathbb{Z}^n$ και θεωρούμε το σύνολο*

$$\Lambda = \{u \in \mathbb{Z}^n : h \equiv qr \bmod m \ \text{ για κάποιον } q \in \mathbb{Z}\}.$$

Τότε το Λ είναι πλέγμα, και $\det(\Lambda) = m^{n-1}$. Επιπλέον, υπάρχουν θετικοί πραγματικοί αριθμοί $\lambda_1, \dots, \lambda_n$ τέτοιοι ώστε

$$\lambda_1 \cdots \lambda_n \leqslant 4^n m^{n-1}$$

και γραμμικά ανεξάρτητα διανύσματα $b_1, \dots, b_n \in \Lambda$, $b_j = (b_{1,j}, \dots, b_{n,j})$, ώστε $|b_{i,j}| \leqslant \frac{\lambda_j}{4}$ για κάθε $i, j = 1, \dots, n$.

Κεφάλαιο 8. Σε αυτό το κεφάλαιο παρουσιάζουμε τα εργαλεία που χρειαζόμαστε από την Θεωρία Γραφημάτων. Με τον όρο *κατευθυνόμενο διμερές γράφημα* εννοούμε μια τριάδα $G = (A, B, E)$, όπου A και B είναι πεπερασμένα σύνολα (όχι κατ' ανάγκην ξένα) και $E \subseteq A \times B$ είναι ένα σύνολο διατεταγμένων ζευγών $(a, b) \in A \times B$. Γράφουμε $G : A \to B$ για να τονίσουμε το

γεγονός ότι τα ζεύγη είναι διατεταγμένα (το γράφημα είναι κατευθυνόμενο). Ο συμβολισμός $a \mapsto_G b$ σημαίνει ότι $(a,b) \in E$. Για κάθε $X \subseteq A$ ορίζουμε $G(X) = \{b \in B : a \mapsto_G b \text{ για κάποιο } a \in X\}$.

Ο *λόγος μεγέθυνσης* $\|G\|$ του G είναι η ποσότητα

$$\|G\| = \min\left\{\frac{|G(X)|}{|X|} : X \subseteq A, X \neq \emptyset\right\}.$$

Ισοδύναμα, $\|G\|$ είναι ο μικρότερος αριθμός για τον οποίο ισχύει $|G(X)| \geqslant \|G\|\,|X|$ για κάθε $X \subseteq A$.

Αν $G : A \to B$ και $H : B \to C$ είναι δύο κατευθυνόμενα διμερή γραφήματα και τα A, B, C είναι ξένα, η *σύνθεση* $H \circ G : A \to C$ είναι το κατευθυνόμενο διμερές γράφημα που ορίζεται ως εξής: $a \mapsto_{H\circ G} c$ αν και μόνο αν υπάρχει $b \in B$ ώστε $a \mapsto_G b$ και $b \mapsto_H c$.

Εισάγουμε την έννοια του γραφήματος Plünnecke. Αν A_0, A_1, A_2 είναι πεπερασμένα υποσύνολα μιας αβελιανής ομάδας G, λέμε ότι δύο διατεταγμένα διμερή γραφήματα $G_1 : A_0 \to A_1$ και $G_2 : A_1 \to A_2$ αντιμετατίθενται αν ισχύει το εξής: αν $a, b, c \in G$ και $a \mapsto_{G_1} a + b \mapsto_{G_2} a + b + c$, τότε $a \mapsto_{G_1} a + c \mapsto_{G_2} a + b + c$. Ένας τρόπος να σκεφτόμαστε αυτή την ιδιότητα είναι ο εξής: αν δύο δαδοχικές ακμές ενός παραλληλογράμμου βρίσκονται στο $G_1 \cup G_2$ τότε το ίδιο ισχύει και για τις άλλες δύο ακμές του παραλληλογράμμου. Γενικότερα, για κάθε $k \geqslant 2$, αν $A_0, A_1, \ldots, A_k$ είνα πεπερασμένα υποσύνολα της G λέμε ότι μια k-άδα $(G_1, \ldots, G_k)$ γραφημάτων $G_j : A_{j-1} \to A_j$ είναι *γράφημα Plünnecke τάξης* k αν για κάθε $j = 1, \ldots, k-1$ τα γραφήματα G_j, G_{j+1} αντιμετατίθενται. Χρειαζόμαστε το θεώρημα Plünnecke:

Θεώρημα 1.3.5 (θεώρημα Plünnecke)**.** *Έστω $(G_1, \ldots, G_k)$ ένα γράφημα Plünnecke τάξης k. Τότε, η ακολουθία των λόγων μεγέθυνσης $\|G_i \circ \cdots \circ G_1\|^{1/i}$, $i = 1, \ldots, k$, είναι φθίνουσα. Ειδικότερα,*

$$\|G_k \circ \cdots \circ G_1\| \leqslant \|G_1\|^k.$$

Για την απόδειξη της ανισότητας Plünnecke αρκεί να δείξουμε ότι: αν $1 \leqslant i < k$ τότε

$$\|G_k \circ \cdots \circ G_1\|^{1/k} \leqslant \|G_i \circ \cdots \circ G_1\|^{1/i}.$$

Σαν πρώτο βήμα για την απόδειξη αυτής της ανισότητας δείχνουμε πρώτα την ακόλουθη «κανονικοποιημένη» μορφή της: Αν $(G_1, \ldots, G_k)$ είναι ένα γράφημα Plünnecke τάξης k ώστε $\|G_k \circ \cdots \circ G_1\| \geqslant 1$, τότε

$$\|G_i \circ \cdots \circ G_1\| \geqslant 1, \quad 1 \leqslant i < k.$$

Η απόδειξη αυτής της ανισότητας βασίζεται στο θεώρημα του Menger.

Ένα τυπικό παράδειγμα γραφήματος Plünnecke, το οποίο θα παίξει ρόλο στη μελέτη μας, είναι το εξής: Έστω A και B πεπερασμένα υποσύνολα μιας αβελιανής ομάδας G. Ορίζουμε $G_{A,B} : A \to A + B$ θέτοντας $a \mapsto_{G_{A,B}} a + b$ αν και μόνο αν $a \in A$ και $b \in B$. Τότε,

$$\|G_{A,B}\| = \min\left\{\frac{|X + A|}{|X|} : X \subseteq A,\ X \neq \emptyset\right\} \leqslant \frac{|A + B|}{|A|}.$$

Παρατηρήστε ότι, αν A, B και C είναι υποσύνολα της G και τα $A, A + B, A + B + C$ είναι ξένα, τότε

$$G_{A+B,C} \circ G_{A,B} = G_{A,B+C}.$$

Η k-άδα $(G_{A,B}, G_{A+B,B}, \ldots, G_{A+(k-1)B,B})$ είναι γράφημα Plünnecke.

Εφαρμόζοντας το θεώρημα Plünnecke στην k-άδα $(G_{A,B}, G_{A+B,B}, \ldots, G_{A+(k-1)B,B})$ παίρνουμε το εξής:

Θεώρημα 1.3.6 (ανισότητα Plünnecke)**.** *Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G που ικανοποιούν την $|A+B| \leqslant c_1|A|$. Τότε, για κάθε $k \in \mathbb{N}$ υπάρχει $X \subseteq A$ ώστε*

$$|X + kB| \leqslant c_1^k |X|.$$

Ειδικότερα,

$$|kB| \leqslant c_1^k |A|.$$

Από αυτήν την ανισότητα και από την τριγωνική ανισότητα του Ruzsa έπεται το θεώρημα Plünnecke–Ruzsa:

Θεώρημα 1.3.7 (θεώρημα Plünnecke–Ruzsa)**.** *Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G ώστε $|A+B| \leqslant c_1|A|$. Τότε,*

$$|nB - mB| \leqslant c_1^{n+m}|A|$$

για κάθε $n, m \geqslant 1$. Ειδικότερα, αν $|A \pm A| \leqslant c_1|A|$ τότε $|nA - nA| \leqslant c_1^{2n}|A|$ για κάθε $n \geqslant 1$.

Αυτή η ανισότητα θα μας χρειαστεί στο τελευταίο κεφάλαιο.

Κεφάλαιο 9. Ο Ruzsa γενίκευσε το θεώρημα του Freiman στο πλαίσιο τυχούσας αβελιανής ομάδας που είναι ελεύθερη στρέψης. Αν $a, q_1, \ldots, q_n$ είναι στοιχεία μιας αβελιανής ομάδας G και $\ell_1, \ldots, \ell_n$ θετικοί ακέραιοι, τότε ο σύνολο

$$Q = Q(a; q_1, \ldots, q_n; \ell_1, \ldots, \ell_n) = \{a + x_1 q_1 + \cdots + x_n q_n : 0 \leqslant x_i < \ell_i\}$$

ονομάζεται n-διάστατη αριθμητική πρόοδος στην G. Το μήκος της Q είναι ο $\ell(Q) = \ell_1 \cdots \ell_n$. Με αυτόν τον ορισμό, το θεώρημα του Ruzsa διατυπώνεται ως εξής:

Θεώρημα 1.3.8 (Ruzsa)**.** *Έστω c, c_1 και c_2 θετικοί πραγματικοί αριθμοί. Έστω $k \geqslant 1$, και έστω A και B πεπερασμένα υποσύνολα μιας ελεύθερης στρέψης αβελιανής ομάδας G, τέτοια ώστε*

$$c_1 k \leqslant |A|, |B| \leqslant c_2 k$$

και

$$|A + B| \leqslant ck.$$

Τότε, το A εριέχεται σε μια n-διάστατη αριθμητική πρόοδο στην G, μήκους το πολύ ℓk, όπου οι n και ℓ εξαρτώνται μόνο από τις σταθερές c, c_1 και c_2.

Παρουσιάζουμε την απόδειξη αυτού του αποτελέσματος. Το θεώρημα του Freiman είναι ειδική περίπτωση: αρκεί να πάρουμε A ένα πεπερασμένο σύνολο ακεραίων και $B = A$.

Βασικό ρόλο στην απόδειξη παίζει η έννοια του *ισομορφισμού Freiman*: Έστω G και H αβελιανές ομάδες, και έστω $A \subseteq G$ και $B \subseteq H$. Έστω $h \geqslant 2$. Μια απεικόνιση $\varphi : A \to B$ λέγεται *ομοιομορφισμός Freiman τάξης h* αν

$$\varphi(a_1) + \cdots + \varphi(a_h) = \varphi(a'_1) + \cdots + \varphi(a'_h)$$

για κάθε $a_1, \dots, a_h, a'_1, \dots, a'_h \in A$ που ικανοποιούν την $a_1 + \cdots + a_h = a'_1 + \cdots + a'_h$. Τότε, η απεικόνιση $\varphi^{(h)} : hA \to hB$ με

$$\varphi^{(h)}(a_1 + \cdots + a_h) = \varphi(a_1) + \cdots + \varphi(a_h)$$

είναι καλά ορισμένη. Αν η $\varphi : A \to B$ είναι ένα προς ένα και επί, και ισχύει ότι $a_1 + \cdots + a_h = a'_1 + \cdots + a'_h$ αν και μόνο αν $\varphi(a_1) + \cdots + \varphi(a_h) = \varphi(a'_1) + \cdots + \varphi(a'_h)$, τότε η φ λέγεται *ισομορφισμός Freiman τάξης* h και η $\varphi^{(h)} : A \to B$ είναι επίσης ένα προς ένα και επί. Ένα ενδιάμεσο βήμα για την απόδειξη του θεωρήματος του Ruzsa είναι το εξής.

Θεώρημα 1.3.9 (Ruzsa)**.** *Έστω W ένα πεπερασμένο σύνολο ακεραίων. Έστω $h \geqslant 2$ και $D = D_{h,h}(W) = hW - hW$. Για κάθε*

$$m \geqslant 4h|D_{h,h}(W)| = 4h|D|$$

υπάρχει σύνολο $W' \subseteq W$ τέτοιο ώστε

$$|W'| \geqslant \frac{|W|}{h}$$

το οποίο είναι Freiman ισομορφικό, τάξης h, με ένα σύνολο κλάσεων ισοτιμίας mod n.

Στην τελευταία παράγραφο αυτού του κεφαλαίου δίνουμε μια εφαρμογή του θεωρήματος του Freiman. Δείχνουμε ότι αν A είναι ένα αρκετά μεγάλο σύνολο ακεραίων (ή, γενικότερα, στοιχείων μιας ελεύθερης στρέψης αβελιανής ομάδας) τέτοιο ώστε $|2A| \leqslant c|A|$ τότε το A περιέχει αρκετά μεγάλη αριθμητική πρόοδο. Η ακριβής διατύπωση είναι η ακόλουθη.

Θεώρημα 1.3.10. *Έστω $c \geqslant 2$ και $t \geqslant 3$. Υπάρχει ακέραιος $k_0(c,t)$ τέτοιος ώστε αν A είναι ένα υποσύνολο μιας ελεύθερης στρέψης αβελιανής ομάδας G με $|A| \geqslant k_0(c,t)$ και $|2A| \leqslant c|A|$, τότε το A περιέχει μια αριθμητική πρόοδο μήκους μεγαλύτερου ή ίσου από t.*

Για την απόδειξη, εκτός από το θεώρημα του Freiman, χρησιμοποιούμε το διάσημο θεώρημα του Szemerédi: για κάθε $\delta > 0$ και $t \geqslant 3$ υπάρχει φυσικός $\ell_0(\delta, t)$ τέτοιος ώστε αν $\ell \geqslant \ell_0(\delta, t)$ και A είναι ένα υποσύνολο του $[0, \ell - 1]$ με $|A| \geqslant \delta\ell$, τότε το A περιέχει αριθμητική πρόοδο μήκους t.

Μέρος I

Το πρόβλημα του **Waring**

ΚΕΦΑΛΑΙΟ 2

Το θεώρημα Hilbert-Waring

2.1 Πολυωνυμικές ταυτότητες και μια εικασία του Hurwitz

Το πρόβλημα του Waring για τον εκθέτη k ζητάει να δείξουμε ότι κάθε μη αρνητικός ακέραιος γράφεται ως άθροισμα φραγμένου πλήθους k-οστών δυνάμεων. Συμβολίζουμε με $g(k)$ τον μικρότερο φυσικό s με την ιδιότητα ότι κάθε μη αρνητικός ακέραιος γράφεται ως άθροισμα ακριβώς s k-οστών δυνάμεων μη αρνητικών ακεραίων. Το πρόβλημα του Waring ζητάει να δείξουμε ότι ο $g(k)$ είναι πεπερασμένος. Αυτό αποδείχθηκε από τον Hilbert το 1909. Σε αυτό το κεφάλαιο παρουσιάζουμε την απόδειξη αυτού του θεωρήματος.

Γνωρίζουμε ότι το πρόβλημα του Waring έχει καταφατική απάντηση όταν $k = 2$ ή $k = 3$. Άλλες περιπτώσεις του προβλήματος ελέγχονται από αυτές τις δύο περιπτώσεις, με τη βοήθεια κάποιων πολυωνυμικών ταυτοτήτων. Δίνουμε εδώ τρία τέτοια παραδείγματα. Σε ό,τι ακολουθεί χρησιμοποιούμε το συμβολισμό

$$(x_1 \pm x_2 \pm \cdots \pm x_r)^k = \sum_{\varepsilon_2,\ldots,\varepsilon_r=\pm 1} (x_1 + \varepsilon_2 x_2 + \cdots + \varepsilon_r x_r)^k.$$

Θεώρημα 2.1.1 (Liouville)**.** *Ισχύει η ταυτότητα*

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2 = \frac{1}{6} \sum_{1 \leqslant i < j \leqslant 4} (x_i + x_j)^4 + \frac{1}{6} \sum_{1 \leqslant i < j \leqslant 4} (x_i - x_j)^4$$

και κάθε μη αρνητικός ακέραιος γράφεται ως άθροισμα 53 *τέταρτων δυνάμεων, δηλαδή,*

$$g(4) \leqslant 53.$$

Απόδειξη. Αρχικά παρατηρούμε ότι

$$(x_1 \pm x_2)^4 = (x_1 + x_2)^4 + (x_1 - x_2)^4 = 2x_1^4 + 12x_1^2x_2^2 + 2x_2^4$$

και έτσι

$$\sum_{1 \leqslant i < j \leqslant 4} (x_i \pm x_j)^4 = \sum_{1 \leqslant i < j \leqslant 4} (x_i + x_j)^4 + \sum_{1 \leqslant i < j \leqslant 4} (x_i - x_j)^4$$

$$= \sum_{1\leqslant i<j\leqslant 4} (2x_i^4 + 12x_i^2x_j^2 + 2x_j^4) = 6\sum_{i=1}^{4} x_i^4 + 12 \sum_{1\leqslant i<j\leqslant 4} x_i^2x_j^2$$
$$= 6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2.$$

Έτσι αποδείχτηκε η ταυτότητα του Liouville. Έστω α ένας μη αρνητικός ακέραιος αριθμός. Από το θεώρημα του Lagrange γνωρίζουμε ότι ο α γράφεται ως άθροισμα 4 τέλειων τετραγώνων, έστω $\alpha = x_1^2 + x_2^2 + x_3^2 + x_4^2$, και έτσι για τον $6\alpha^2$ έχουμε ότι ο

$$6\alpha^2 = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) = \sum_{1\leqslant i<j\leqslant 4} (x_i + x_j)^4 + \sum_{1\leqslant i<j\leqslant 4} (x_i - x_j)^4$$

γράφεται ως άθροισμα 12 τετάρτων δυνάμεων. Κάθε μη αρνητικός ακέραιος n μπορεί να γραφεί στην μορφή $n = 6q + r$, με $q \geqslant 0$ και $0 \leqslant r \leqslant 5$. Πάλι από το θεώρημα του Lagrange προκύπτει ότι $q = a_1^2 + \cdots + a_4^2$ και συνεπώς ο $6q = 6a_1^2 + \cdots + 6a_4^2$ είναι το άθροισμα 48 τετάρτων δυνάμεων. Καθώς όμως ο r είναι το άθροισμα 5 τετάρτων δυνάμεων, κάθε μία εκ των οποίων είναι ίση με 0^4 ή 1^4, συμπεραίνουμε ότι ο n είναι το άθροισμα 53 τετάρτων δυνάμεων. □

Οι αποδείξεις των επόμενων δύο αποτελεσμάτων είναι παρόμοιες.

Θεώρημα 2.1.2 (Fleck)**.** *Ισχύει η ταυτότητα*

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)^3 = \frac{1}{60} \sum_{1\leqslant i<j<k\leqslant 4} (x_i \pm x_j \pm x_k)^6 + \frac{1}{30} \sum_{1\leqslant i<j\leqslant 4} (x_i \pm x_j)^6 + \frac{3}{5} \sum_{1\leqslant i\leqslant 4} x_i^6$$

και κάθε μη αρνητικός ακέραιος γράφεται ως άθροισμα πεπερασμένου πλήθους έκτων δυνάμεων.

Θεώρημα 2.1.3 (Hurwitz)**.** *Ισχύει η ταυτότητα*

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)^4 = \frac{1}{840}(x_1 \pm x_2 \pm x_3 \pm x_4)^8 + \frac{1}{5040} \sum_{1\leqslant i<j<k\leqslant 4} (2x_i \pm x_j \pm x_k)^8$$
$$+ \frac{1}{84} \sum_{1\leqslant i<j\leqslant 4} (x_i \pm x_j)^8 + \frac{1}{840} \sum_{1\leqslant i\leqslant 4} (2x_i)^8$$

και κάθε μη αρνητικός ακέραιος γράφεται ως άθροισμα πεπερασμένου πλήθους όγδοων δυνάμεων.

Ας υποθέσουμε ότι

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)^k = \sum_{i=1}^{M} a_i(b_{i,1}x_1^2 + b_{i,2}x_2^2 + b_{i,3}x_3^2 + b_{i,4}x_4^2)^{2k} \tag{2.1.1}$$

για κάποιον θετικό ακέραιο M, κάποιους ακεραίους $b_{i,j}$ και κάποιους θετικούς ρητούς αριθμούς a_i. Ο Hurwitz παρατήρησε ότι από αυτήν την πολυωνυμική ταυτότητα και από το θεώρημα του Lagrange προκύπτει άμεσα ότι αν το πρόβλημα του Waring έχει καταφατική απάντηση για τον εκθέτη k τότε το ίδιο ισχύει και για τον εκθέτη $2k$. Στη συνέχεια, ο Hilbert απέδειξε ότι πολυωνυμικές ταυτότητες της μορφής (2.1.1) ισχύουν για όλους τους θετικούς ακεραίους k, και εφάρμοσε αυτό το αποτέλεσμα για να απαντήσει στο πρόβλημα του Waring για κάθε εκθέτη k. Αυτή ήταν η πρώτη πλήρης απάντηση που δόθηκε στο πρόβλημα του Waring. Στην επόμενη παράγραφο θα δούμε πώς αποδεικνύονται οι πολυωνυμικές ταυτότητες του Hilbert.

2.2 Πολυώνυμα Hermite και η ταυτότητα του Hilbert

Για κάθε $n \geqslant 0$ ορίζουμε το *πολυώνυμο Hermite* $H_n(x)$ ως εξής:

$$H_n(x) = \Big(-\frac{1}{2}\Big)^n e^{x^2} \frac{d^n}{dx^n}(e^{-x^2}).$$

Τα πρώτα πέντε πολυώνυμα Hermite είναι τα:

$$\begin{aligned} H_0(x) &= 1 \\ H_1(x) &= x \\ H_2(x) &= x^2 - \frac{1}{2} \\ H_3(x) &= x^3 - \frac{3}{2}x \\ H_4(x) &= x^4 - 3x^2 + \frac{3}{4}. \end{aligned}$$

Παρατηρούμε ότι

$$\begin{aligned} H_n'(x) &= \Big(-\frac{1}{2}\Big)^n \frac{d}{dx}\Big(e^{x^2} \frac{d^n}{dx^n}(e^{-x^2})\Big) \\ &= \Big(-\frac{1}{2}\Big)^n (2x) e^{x^2} \frac{d^n}{dx^n}(e^{-x^2}) - 2\Big(-\frac{1}{2}\Big)^{n+1} e^{x^2} \frac{d^{n+1}}{dx^{n+1}}(e^{-x^2}) \\ &= 2xH_n(x) - 2H_{n+1}(x), \end{aligned}$$

δηλαδή τα πολυώνυμα Hermite ικανοποιούν την αναδρομική σχέση

$$H_{n+1}(x) = xH_n(x) - \frac{1}{2}H_n'(x). \tag{2.2.1}$$

Έπεται ότι το $H_n(x)$ είναι μονικό πολυώνυμο βαθμού n με ρητούς συντελεστές και ότι το $H_n(x)$ είναι άρτιο πολυώνυμο όταν ο n είναι άρτιος και περιττό πολυώνυμο όταν ο n είναι περιττός.

Λήμμα 2.2.1. *Το n-οστό πολυώνυμο Hermite $H_n(x)$ έχει n διακεκριμένες πραγματικές ρίζες.*

Απόδειξη. Με επαγωγή στο n. Το λήμμα είναι φανερό για $n = 0$ και $n = 1$, καθώς $H_0(x) = 1$ και $H_1(x) = x$. Έστω $n \geqslant 1$, και ας υποθέσουμε ότι το λήμμα ισχύει για τον n. Τότε το $H_n(x)$ έχει n το πλήθος διαφορετικές μεταξύ τους πραγματικές ρίζες, οι οποίες θα είναι και απλές. Αυτό σημαίνει ότι υπάρχουν πραγματικοί αριθμοί

$$\beta_n < \cdots < \beta_2 < \beta_1$$

τέτοιοι ώστε

$$H_n(\beta_j) = 0$$

και

$$H_n'(\beta_j) \neq 0$$

για $j = 1, \ldots, n$. Καθώς το $H_n(x)$ είναι μονικό πολυώνυμο βαθμού n, προκύπτει ότι

$$\lim_{x \to \infty} H_n(x) = \infty,$$

και έτσι

$$H_n'(\beta_1) > 0.$$

Από το θεώρημα του Rolle προκύπτει ότι κάθε ένα από τα διαστήματα (β_j, β_{j-1}) για $j = 2, \ldots, n$ περιέχει ακριβώς μία από τις $n-1$ το πλήθος ρίζες του πολυωνύμου $H_n'(x)$. Από αυτό εύκολα προκύπτει ότι

$$(-1)^{j+1} H_n'(\beta_j) > 0$$

για $j = 1, \ldots, n$. Από την αναδρομική σχέση $H_{n+1}(x) = xH_n(x) - \frac{1}{2}H_n'(x)$ θέτοντας $x = \beta_j$ έχουμε ότι

$$H_{n+1}(\beta_j) = -\frac{1}{2} H_n'(\beta_j),$$

και έτσι

$$(-1)^j H_{n+1}(\beta_j) = \frac{(-1)^{j+1}}{2} H_n'(\beta_j) > 0$$

για $j = 1, \ldots, n$. Εφαρμόζοντας τώρα το θεώρημα Bolzano σε καθένα από τα κλειστά διαστήματα $[\beta_j, \beta_{j-1}]$ για $j = 2, \ldots, n$, παίρνουμε ότι το πολυώνυμο $H_{n+1}(x)$ έχει μία ρίζα β_j^* σε καθένα από τα διαστήματα (β_j, β_{j-1}). Επίσης, καθώς $\lim_{x\to\infty} H_{n+1}(x) = \infty$ και $H_{n+1}(\beta_1) < 0$, βλέπουμε ότι το πολυώνυμο $H_{n+1}(x)$ έχει μία ρίζα $\beta_1^* > \beta_1$. Αν τώρα ο n είναι άρτιος, $H_{n+1}(\beta_n) > 0$. Επιπλέον ο $n+1$ έιναι περιττός αριθμός και συνεπώς για το H_{n+1} το οποίο είναι πολυώνυμο περιττού βαθμού ισχύει ότι $\lim_{x\to\infty} H_{n+1}(x) = -\infty$. Πάλι από το θεώρημα Bolzano παίρνουμε ότι το $H_{n+1}(x)$ έχει μία ρίζα $\beta_{n+1}^* < \beta_n$. Με ανάλογο συλλογισμό προκύπτει ότι το $H_{n+1}(x)$ έχει μία ρίζα $\beta_{n+1}^* < \beta_n$ αν ο n ειναι περιττος. Σε κάθε περίπτωση λοιπόν, το $H_{n+1}(x)$ έχει $n+1$ το πλήθος και διαφορετικές μεταξύ τους πραγματικές ρίζες. □

Λήμμα 2.2.2. *Έστω $n \geqslant 1$ και $f(x)$ ένα πολυώνυμο βαθμού μικρότερου ή ίσου από $n-1$. Τότε,*

$$\int_{-\infty}^{\infty} e^{-x^2} H_n(x) f(x)\, dx = 0.$$

Απόδειξη. Με επαγωγή ως προς n. Αν $n = 1$ τότε $H_1(x) = x$ και η $f(x)$ είναι σταθερή, ας πούμε $f(x) = a_0$, άρα

$$\int_{-\infty}^{\infty} e^{-x^2} H_1(x) f(x)\, dx = a_0 \int_{-\infty}^{\infty} e^{-x^2} x\, dx = 0.$$

Υποθέτουμε ότι το συμπέρασμα του λήμματος ισχύει για τον n, και θεωρούμε ένα πολυώνυμο $f(x)$ βαθμού το πολύ n. Τότε, το $f'(x)$ είναι πολυώνυμο βαθμού το πολύ $n-1$. Ολοκληρώνοντας κατά μέρη, παίρνουμε

$$\begin{aligned}
\int_{-\infty}^{\infty} e^{-x^2} H_{n+1}(x) f(x)\, dx &= \Big(-\frac{1}{2}\Big)^{n+1} \int_{-\infty}^{\infty} \frac{d^{n+1}}{dx^{n+1}}(e^{-x^2}) f(x)\, dx \\
&= \Big(-\frac{1}{2}\Big)^{n+1} \int_{-\infty}^{\infty} \frac{d^{n}}{dx^{n}}(e^{-x^2}) f'(x)\, dx \\
&= -\frac{1}{2} \int_{-\infty}^{\infty} e^{-x^2} H_n(x) f'(x)\, dx \\
&= 0,
\end{aligned}$$

όπως θέλαμε. □

Λήμμα 2.2.3. *Για κάθε άρτιο $n \geqslant 0$ ισχύει*

$$c_n = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} x^n \, dx = \frac{n!}{2^n (n/2)!}, \tag{2.2.2}$$

ενώ αν ο $n > 0$ είναι περιττός τότε $c_n = 0$.

Απόδειξη. Με επαγωγή ως προς n. Για $n = 0$ έχουμε

$$\int_{-\infty}^{\infty} e^{-x^2} dx = \sqrt{\pi},$$

άρα $c_0 = 1$. Για $n = 1$, η συνάρτηση $e^{-x^2} x$ είναι περιττή, άρα

$$\int_{-\infty}^{\infty} e^{-x^2} x \, dx = 0$$

και $c_1 = 0$. Έστω τώρα $n \geqslant 2$, και ας υποθέσουμε ότι το λήμμα ισχύει για τον $n-2$. Έχουμε

$$\int_0^{\infty} e^{-x^2} x^n \, dx = -\frac{1}{2} \int_0^{\infty} \frac{d}{dx}(e^{-x^2}) x^{n-1} \, dx$$

και τώρα ολοκληρώνοντας κατά μέρη παίρνουμε

$$\int_0^{\infty} \frac{d}{dx}(e^{-x^2}) x^{n-1} \, dx = \left[e^{-x^2} x^{n-1} \right]_0^{\infty} - (n-1) \int_0^{\infty} e^{-x^2} x^{n-2} \, dx = -(n-1) \int_0^{\infty} e^{-x^2} x^{n-2} \, dx$$

καθώς $\lim_{x \to \infty} (e^{-x^2} x^{n-1}) = 0$. Έτσι

$$\int_0^{\infty} e^{-x^2} x^n \, dx = \frac{n-1}{2} \int_0^{\infty} e^{-x^2} x^{n-2} \, dx$$

Αντίστοιχα

$$\int_{-\infty}^{0} e^{-x^2} x^n \, dx = \frac{n-1}{2} \int_{-\infty}^{0} e^{-x^2} x^{n-2} \, dx.$$

Συνεπώς,

$$c_n = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} x^n \, dx = \frac{n-1}{2} \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} x^{n-2} \, dx = \frac{n-1}{2} c_{n-2}.$$

Αν ο n είναι περιττός, τότε $c_{n-2} = 0$ άρα $c_n = 0$. Αν ο n είναι άρτιος, τότε

$$c_n = \frac{n-1}{2} c_{n-2} = \frac{n-1}{2} \frac{(n-2)!}{2^{n-2}((n-2)/2)!} = \frac{n!}{2^n (n/2)!}.$$

Έπεται το λήμμα. □

Λήμμα 2.2.4. *Έστω $n \geqslant 1$ και $\beta_1, \ldots, \beta_n$ διακεκριμένοι πραγματικοί αριθμοί. Αν $c_0, c_1, \ldots, c_{n-1}$ είναι οι σταθερές που ορίστηκαν στην (2.2.2) τότε το σύστημα γραμμικών εξισώσεων*

$$\sum_{j=1}^{n} \beta_j^k x_j = c_k, \qquad k = 0, 1, \ldots, n-1 \tag{2.2.3}$$

έχει μοναδική λύση $\varrho_1, \ldots, \varrho_n$. Για κάθε πολυώνυμο $r(x)$ βαθμού μικρότερου ή ίσου από $n-1$ ισχύει

$$\sum_{j=1}^{n} r(\beta_j) \varrho_j = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} r(x) \, dx.$$

Απόδειξη. Η ύπαρξη και η μοναδικότητα της λύσης $\varrho_1, \ldots, \varrho_n$ προκύπτει άμεσα από το γεγονός ότι η ορίζουσα του συστήματος γραμμικών εξισώσεων

$$\begin{aligned} x_1 + x_2 + \cdots + x_n &= c_0 \\ \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n &= c_1 \\ \beta_1^2 x_1 + \beta_2^2 x_2 + \cdots + \beta_n^2 x_n &= c_2 \\ &\vdots \\ \beta_1^{n-1} x_1 + \beta_2^{n-1} x_2 + \cdots + \beta_n^{n-1} x_n &= c_{n-1} \end{aligned}$$

είναι η ορίζουσα Vandermonde

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \beta_1 & \beta_2 & \ldots & \beta_n \\ \beta_1^2 & \beta_2^2 & \ldots & \beta_n^2 \\ \vdots & & & \vdots \\ \beta_1^{n-1} & \beta_2^{n-1} & \ldots & \beta_n^{n-1} \end{vmatrix} = \prod_{0 \leqslant i < j \leqslant n} (\beta_j - \beta_i) \neq 0$$

Για το πολυώνυμο $r(x) = \sum_{k=0}^{n-1} a_k x^k$ βαθμού το πολύ $n-1$ έχουμε

$$\begin{aligned} \sum_{j=1}^{n} r(\beta_j)\varrho_j &= \sum_{j=1}^{n} \sum_{k=0}^{n-1} a_k \beta_j^k \varrho_j \\ &= \sum_{k=0}^{n-1} a_k \sum_{j=1}^{n} \beta_j^k \varrho_j \\ &= \sum_{k=0}^{n-1} a_k c_k \\ &= \frac{1}{\sqrt{\pi}} \sum_{k=0}^{n-1} a_k \int_{-\infty}^{\infty} e^{-x^2} x^k dx \\ &= \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} r(x) dx. \end{aligned}$$

□

Λήμμα 2.2.5. *Έστω $n \geqslant 1$ και $\beta_1, \ldots, \beta_n$ οι n διακεκριμένες πραγματικές ρίζες του n-οστού πολυωνύμου Hermite $H_n(x)$. Αν $\varrho_1, \ldots, \varrho_n$ είναι η λύση του συστήματος γραμμικών εξισώσεων* (2.2.3) *τότε, για κάθε πολυώνυμο $f(x)$ βαθμού το πολύ $2n-1$,*

$$\sum_{j=1}^{n} f(\beta_j)\varrho_j = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} f(x) dx.$$

Απόδειξη. Από τον αλγόριθμο της διαίρεσης πολυωνύμων, μπορούμε να βρούμε πολυώνυμα $q(x)$ και $r(x)$ βαθμού το πολύ $n-1$ τέτοια ώστε

$$f(x) = H_n(x)q(x) + r(x).$$

Αφού $H_n(\beta_j) = 0$ για κάθε $j = 1, \ldots, n$, έχουμε

$$f(\beta_j) = H_n(\beta_j)q(\beta_j) + r(\beta_j) = r(\beta_j).$$

Από το Λήμμα 2.2.4 και το Λήμμα 2.2.2,

$$\begin{aligned}\sum_{j=1}^{n} f(\beta_j)\varrho_j &= \sum_{j=1}^{n} r(\beta_j)\varrho_j \\ &= \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} r(x)\, dx \\ &= \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} H_n(x)q(x)\, dx + \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} r(x)\, dx \\ &= \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} f(x)\, dx,\end{aligned}$$

και έχουμε το ζητούμενο. □

Λήμμα 2.2.6. *Έστω $n \geqslant 1$ και $\beta_1, \ldots, \beta_n$ οι n διακεκριμένες πραγματικές ρίζες του n-οστού πολυωνύμου Hermite $H_n(x)$. Αν $\varrho_1, \ldots, \varrho_n$ είναι η λύση του συστήματος γραμμικών εξισώσεων (2.2.3) τότε $\varrho_i > 0$ για κάθε $i = 1, \ldots, n$.*

Απόδειξη. Καθώς

$$H_n(x) = \prod_{j=1}^{n} (x - \beta_j),$$

προκύπτει ότι για $i = 1, \ldots, n$, το

$$f_i(x) = \left(\frac{H_n(x)}{x - \beta_i}\right)^2 = \prod_{j=1, j\neq i}^{n} (x - \beta_j)^2$$

είναι ένα μονικό πολυώνυμο βαθμού $2n - 2$ τέτοιο ώστε $f_i(x) \geqslant 0$ για κάθε x. Έτσι έχουμε

$$\frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} f_i(x) dx > 0.$$

Όμως $f_i(\beta_i) > 0$ και $f_i(\beta_j) = 0$ για $i \neq j$. Έτσι από το Λήμμα 2.2.5 παίρνουμε ότι

$$f_i(\beta_i)\varrho_i = \sum_{j=1}^{n} f_i(\beta_j)\varrho_j = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} f_i(x) dx > 0,$$

και έτσι έχουμε το ζητούμενο. □

Λήμμα 2.2.7. *Έστω $n \geqslant 1$ και $c_0, c_1, \ldots, c_{n-1}$ οι ρητοί αριθμοί που ορίζονται από την (2.2.2). Υπάρχουν διακεκριμένοι ρητοί αριθμοί $\beta_1^*, \ldots, \beta_n^*$ και θετικοί ρητοί αριθμοί $\varrho_1^*, \ldots, \varrho_n^*$ τέτοιοι ώστε*

$$\sum_{j=1}^{n} (\beta_j^*)^k \varrho_j^* = c_k$$

για κάθε $k = 0, 1, \ldots, n - 1$.

Απόδειξη. Από το Λήμμα 2.2.4, για κάθε n-αδα διακεκριμένων πραγματικών αριθμών $\beta_1, \beta_2, \ldots, \beta_n$ το σύστημα των n γραμμικων εξισώσεων με n αγνώστους

$$\sum_{j=1}^{n} \beta_j^k x_j = c_k \qquad k = 0, 1, \ldots, n-1$$

έχει μοναδική λύση $(\varrho_1, \varrho_2, \ldots, \varrho_n)$. Έστω $\Re$ το ανοικτό υποσύνολο του $\mathbb{R}^n$ που αποτελείται από όλα τα σημεία $(\beta_1, \beta_2, \ldots, \beta_n)$ με $\beta_i \neq \beta_j$ για $i \neq j$, και έστω επίσης $\Phi : \Re \to \mathbb{R}^n$ η συνάρτηση που στέλνει το $(\beta_1, \beta_2, \ldots, \beta_n)$ στο $(\varrho_1, \varrho_2, \ldots, \varrho_n)$. Από τον κανόνα του Cramer για την επίλυση γραμμικών εξισώσεων, μπορούμε να εκφράσουμε κάθε ϱ_j ως ρητή συνάρτηση των $\beta_1, \beta_2, \ldots, \beta_n$, και έτσι η συνάρτηση

$$\Phi(\beta_1, \beta_2, \ldots, \beta_n) = (\varrho_1, \varrho_2, \ldots, \varrho_n)$$

είναι συνεχής. Έστω $\mathbb{R}^n_+$ το ανοικτό υποσύνολο του $\mathbb{R}^n$ που αποτελείται από όλα τα σημεία $(x_1, x_2, \ldots, x_n)$ με $x_i > 0$ για $i = 1, 2, \ldots, n$. Από το Λήμμα 2.2.6, αν $\beta_1, \beta_2, \ldots, \beta_n$ είναι οι n ρίζες του πολυωνύμου $H_n(x)$, έχουμε ότι $(\beta_1, \beta_2, \ldots, \beta_n) \in \Re$ και

$$\Phi(\beta_1, \beta_2, \ldots, \beta_n) = (\varrho_1, \varrho_2, \ldots, \varrho_n) \in \mathbb{R}^n_+.$$

Καθώς το R^n_+ είναι ανοικτό υποσύνολο του R^n, συμπεραίνουμε ότι το $\Phi^{-1}(\mathbb{R}^n_+)$ είναι μια ανοικτή περιοχή του $(\beta_1, \ldots, \beta_n)$ στο $\Re$. Καθώς τα σημεία με ρητές συντεταγμένες είναι πυκνά στο $\Re$, η περιοχή αυτή περιέχει ένα σημείο $(\beta_1^*, \beta_2^*, \ldots, \beta_n^*)$ με ρητές συντεταγμένες. Θεωρούμε τώρα το σημείο

$$(\varrho_1^*, \varrho_2^*, \ldots, \varrho_n^*) = \Phi(\beta_1^*, \beta_2^*, \ldots, \beta_n^*) \in \mathbb{R}^n_+.$$

Κάθε ένας από τους αριθμούς ϱ_i^* μπορεί να εκφραστεί ως ρητή συνάρτηση των ρητών αριθμών $\beta_1^*, \beta_2^*, \ldots, \beta_n^*$ και άρα είναι φανερό ότι κάθε ένας από τους θετικούς αριθμούς ϱ_i^* είναι ρητός, το οποίο ολοκληρώνει και την απόδειξη του λήμματος. □

Λήμμα 2.2.8. *Έστω $n \geqslant 1$ και $c_0, c_1, \ldots, c_{n-1}$ οι ρητοί αριθμοί που ορίζονται από την* (2.2.2). *Έστω επίσης $\beta_1, \ldots, \beta_n$ διακεκριμένοι πραγματικοί αριθμοί, και $\varrho_1, \ldots, \varrho_n$ η λύση του γραμμικού συστήματος* (2.2.3). *Για κάθε θετικό ακέραιο r και κάθε $m = 1, 2, \ldots, n-1$, ισχύει η πολυωνυμική ταυτότητα*

$$c_m(x_1^2 + \cdots + x_r^2)^{m/2} = \sum_{j_1=1}^{n} \cdots \sum_{j_r=1}^{n} \varrho_{j_1} \cdots \varrho_{j_r} (\beta_{j_1} x_1 + \cdots + \beta_{j_r} x_r)^m.$$

Απόδειξη. Έχουμε

$$\begin{aligned}
&\sum_{j_1=1}^{n}\cdots\sum_{j_r=1}^{n}\varrho_{j_1}\cdots\varrho_{j_r}(\beta_{j_1}x_1+\cdots+\beta_{j_r}x_r)^m\\
&\qquad=\sum_{j_1=1}^{n}\cdots\sum_{j_r=1}^{n}\varrho_{j_1}\cdots\varrho_{j_r}\sum_{\substack{\mu_1+\cdots+\mu_r=m\\ \mu_i\geqslant 0}}\frac{m!}{\mu_1!\cdots\mu_r!}(\beta_{j_1}x_1)^{\mu_1}\cdots(\beta_{j_r}x_r)^{\mu_r}\\
&\qquad=m!\sum_{j_1=1}^{n}\cdots\sum_{j_r=1}^{n}\sum_{\substack{\mu_1+\cdots+\mu_r=m\\ \mu_i\geqslant 0}}\frac{x_1^{\mu_1}}{\mu_1!}(\beta_{j_1}^{\mu_1}\varrho_{j_1})\cdots\frac{x_r^{\mu_r}}{\mu_r!}(\beta_{j_r}^{\mu_r}\varrho_{j_r})\\
&\qquad=m!\sum_{\substack{\mu_1+\cdots+\mu_r=m\\ \mu_i\geqslant 0}}\sum_{j_1=1}^{n}\cdots\sum_{j_r=1}^{n}\prod_{i=1}^{r}\frac{x_i^{\mu_i}}{\mu_i!}(\beta_{j_i}^{\mu_i}\varrho_{j_i})\\
&\qquad=m!\sum_{\substack{\mu_1+\cdots+\mu_r=m\\ \mu_i\geqslant 0}}\prod_{i=1}^{r}\Big(\frac{x_i^{\mu_i}}{\mu_i!}\sum_{j=1}^{n}\beta_j^{\mu_i}\varrho_j\Big)\\
&\qquad=m!\sum_{\substack{\mu_1+\cdots+\mu_r=m\\ \mu_i\geqslant 0}}\prod_{i=1}^{r}\frac{c_{\mu_i}x_i^{\mu_i}}{\mu_i!}.
\end{aligned}$$

Από το Λήμμα 2.2.3 έχουμε $c_m=0$ αν ο m είναι περιττός. Αν ο m είναι περιττός και $\mu_1+\cdots+\mu_r=m$, τότε ο μ_i πρέπει να είναι περιττός για τουλάχιστον έναν δείκτη i, άρα

$$\sum_{j_1=1}^{n}\cdots\sum_{j_r=1}^{n}\varrho_{j_1}\cdots\varrho_{j_r}(\beta_{j_1}x_1+\cdots+\beta_{j_r}x_r)^m=0.$$

Αυτό αποδεικνύει το λήμμα στην περίπτωση που ο m είναι περιττός. Αν ο m είναι άρτιος, τότε αρκεί να θεωρήσουμε μόνο διαμερίσεις του m σε άρτιους $\mu_i=2\nu_i$. Εισάγοντας τους c_n, όπως αυτοί

δίνονται στην (2.2.2), παίρνουμε

$$\begin{aligned}
\sum_{j_1=1}^{n}\cdots\sum_{j_r=1}^{n}\varrho_{j_1}\cdots\varrho_{j_r}(\beta_{j_1}x_1+\cdots+\beta_{j_r}x_r)^m
&= m!\sum_{\substack{2\nu_1+\cdots+2\nu_r=m\\ \nu_i\geqslant 0}}\prod_{i=1}^{r}\frac{c_{2\nu_i}x_i^{2\nu_i}}{(2\nu_i)!}\\
&= m!\sum_{\substack{\nu_1+\cdots+\nu_r=m/2\\ \nu_i\geqslant 0}}\prod_{i=1}^{r}\frac{(2\nu_i)!}{2^{2\nu_i}\nu_i!}\frac{x_i^{2\nu_i}}{(2\nu_i)!}\\
&= \frac{m!}{2^m}\sum_{\substack{\nu_1+\cdots+\nu_r=m/2\\ \nu_i\geqslant 0}}\prod_{i=1}^{r}\frac{x_i^{2\nu_i}}{\nu_i!}\\
&= \frac{m!}{2^m(m/2)!}\,(m/2)!\sum_{\substack{\nu_1+\cdots+\nu_r=m/2\\ \nu_i\geqslant 0}}\prod_{i=1}^{r}\frac{(x_i^2)^{\nu_i}}{\nu_i!}\\
&= c_m\sum_{\substack{\nu_1+\cdots+\nu_r=m/2\\ \nu_i\geqslant 0}}\frac{(m/2)!}{\nu_1!\cdots\nu_r!}(x_1^2)^{\nu_1}\cdots(x_r^2)^{\nu_r}\\
&= c_m(x_1^2+\cdots+x_r^2)^{m/2},
\end{aligned}$$

το οποίο ολοκληρώνει την απόδειξη. □

Θεώρημα 2.2.9 (ταυτότητα του Hilbert)**.** *Για κάθε $k\geqslant 1$ και $r\geqslant 1$ μπορούμε να βρούμε ακέραιο M και θετικούς ρητούς αριθμούς a_i και ακεραίους $b_{i,j}$, για $i=1,\dots,M$ και $j=1,\dots,r$, τέτοιους ώστε*

$$(x_1^2+\cdots+x_r^2)^k=\sum_{i=1}^{M}a_i(b_{i,1}x_1+\cdots+b_{i,r}x_r)^{2k}. \tag{2.2.4}$$

Απόδειξη. Επιλέγουμε $n>2k$ και θεωρούμε τους ρητούς αριθμούς $\beta_1^*,\dots,\beta_n^*,\varrho_1^*,\dots,\varrho_n^*$ που κατασκευάστηκαν στο Λήμμα 2.2.7. Οι $\beta_1^*,\dots,\beta_n^*$ είναι διακεκριμένοι και οι $\varrho_1^*,\dots,\varrho_n^*$ είναι θετικοί. Χρησιμοποιώντας αυτούς τους αριθμούς στο Λήμμα 2.2.8 με $m=2k$ παίρνουμε την πολυωνυμική ταυτότητα

$$c_{2k}(x_1^2+\cdots+x_r^2)^k=\sum_{j_1=1}^{n}\cdots\sum_{j_r=1}^{n}\varrho_{j_1}^*\cdots\varrho_{j_r}^*(\beta_{j_1}^*x_1+\cdots+\beta_{j_r}^*x_r)^{2k}.$$

Έστω q ένας κοινός παρονομαστής των n κλασμάτων $\beta_1^*,\dots,\beta_n^*$. Τότε, ο $q\beta_j^*$ είναι ακέραιος για κάθε j, και η

$$(x_1^2+\cdots+x_r^2)^k=\sum_{j_1=1}^{n}\cdots\sum_{j_r=1}^{n}\frac{\varrho_{j_1}^*\cdots\varrho_{j_r}^*}{c_{2k}q^{2k}}(q\beta_{j_1}^*x_1+\cdots+q\beta_{j_r}^*x_r)^{2k}$$

μας δίνει την πολυωνυμική ταυτότητα τύπου Hilbert που ζητούσαμε. □

Λήμμα 2.2.10. *Έστω $k \geqslant 1$. Αν υπάρχουν θετικοί ρητοί αριθμοί $a_1, \ldots, a_M$ τέτοιοι ώστε κάθε αρκετά μεγάλος φυσικός n να γράφεται στη μορφή*

$$n = \sum_{i=1}^{M} a_i y_i^k \tag{2.2.5}$$

για κάποιους μη αρνητικούς ακεραίους $y_1, \ldots, y_M$, τότε το πρόβλημα του Waring έχει καταφατική απάντηση για τον εκθέτη k.

Απόδειξη. Επιλέγουμε n_0 τέτοιον ώστε κάθε ακέραιος $n \geqslant n_0$ να αναπαρίσταται στη μορφή (2.2.5). Έστω q το ελάχιστο κοινό πολλαπλάσιο των παρονομαστών των κλασμάτων $a_1, \ldots, a_M$. Τότε, $qa_i \in \mathbb{Z}$ για κάθε $i = 1, \ldots, M$, και ο qn είναι το άθροισμα $\sum_{i=1}^{M} qa_i$ μη αρνητικών k-οστών δυνάμεων για κάθε $n \geqslant n_0$. Αφού κάθε ακέραιος $N \geqslant qn_0$ γράφεται στη μορφή $N = qn + r$, όπου $n \geqslant n_0$ και $0 \leqslant r \leqslant q-1$, έπεται ότι ο N γράφεται ως άθροισμα $\sum_{i=1}^{M} qa_i + q - 1$ μη αρνητικών k-οστών δυνάμεων. Δεδομένου ότι κάθε μη αρνητικός ακέραιος $N < qn_0$ γράφεται ως άθροισμα φραγμένου πλήθους k-οστών δυνάμεων, συμπεραίνουμε ότι το πρόβλημα του Waring έχει θετική απάντηση για τον k. □

Στη συνέχεια θα χρησιμοποιούμε τον ακόλουθο συμβολισμό, ο οποίος οφείλεται στον Stridsberg: Έστω $\sum_{i=1}^{M} a_i x_i^k$ δεδομένη διαγώνια μορφή βαθμού k με θετικούς ρητούς συντελεστές $a_1, \ldots, a_M$. Γράφουμε

$$n = \sum(k)$$

αν υπάρχουν μη αρνητικοί ακέραιοι $x_1, \ldots, x_M$ τέτοιοι ώστε

$$n = \sum_{i=1}^{M} a_i x_i^k. \tag{2.2.6}$$

Συμβολίζουμε με $\sum(k)$ κάθε ακέραιο της μορφής (2.2.6). Με αυτόν τον συμβολισμό έχουμε

$$\sum(k) + \sum(k) = \sum(k) \quad \text{και} \quad \sum(2k) = \sum(k).$$

Το Λήμμα 2.2.10 μπορεί τώρα να διατυπωθεί ως εξής: Αν $n = \sum(k)$ για κάθε αρκετά μεγάλο μη αρνητικό ακέραιο n, τότε το πρόβλημα του Waring έχει θετική απάντηση για τον εκθέτη k.

Θεώρημα 2.2.11. *Αν το πρόβλημα του Waring έχει καταφατική απάντηση για τον εκθέτη k τότε έχει καταφατική απάντηση και για τον εκθέτη $2k$.*

Απόδειξη. Χρησιμοποιούμε την ταυτότητα του Hilbert (2.2.4) για τον k με $r = 4$:

$$(x_1^2 + \cdots + x_4^2)^k = \sum_{i=1}^{M} a_i (b_{i,1}x_1 + \cdots + b_{i,4}x_4)^{2k}.$$

Έστω y ένας μη αρνητικός ακέραιος. Από το θεώρημα του Lagrange, υπάρχουν μη αρνητικοί ακέραιοι x_1, x_2, x_3, x_4 τέτοιοι ώστε

$$y = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

άρα

$$y^k = \sum_{i=1}^{M} a_i z_i^{2k}, \tag{2.2.7}$$

όπου οι

$$z_i = b_{i,1}x_1 + \cdots + b_{i,4}x_4$$

είναι μη αρνητικοί ακέραιοι. Αυτό σημαίνει ότι

$$y^k = \sum(2k)$$

για κάθε μη αρνητικό ακέραιο y. Αν το πρόβλημα του Waring έχει θετική απάντηση για τον k, τότε κάθε μη αρνητικός ακέραιος γράφεται ως άθροισμα φραγμένου πλήθους k-οστών δυνάμεων, άρα κάθε μη αρνητικός ακέραιος είναι το άθροισμα φραγμένου πλήθος αριθμών της μορφής $\sum(2k)$. Από το Λήμμα 2.2.10, το πρόβλημα του Waring έχει θετική απάντηση και για τον εκθέτη $2k$. □

2.3 Απόδειξη με επαγωγή

Θα χρησιμοποιήσουμε την ταυτότητα του Hilbert για να δώσουμε καταφατική απάντηση στο πρόβλημα του Waring για όλους τους εκθέτες $k \geqslant 2$. Η απόδειξη θα γίνει με επαγωγή ως προς k. Αφετηρία μας είναι το θεώρημα του Lagrange σύμφωνα με το οποίο κάθε μη αρνητικός ακέραιος είναι το άθροισμα τεσσάρων τετραγώνων. Αυτό αντιστοιχεί στην περίπτωση $k = 2$. Θα αποδείξουμε ότι αν $k > 2$ και το πρόβλημα του Waring έχει καταφατική απάντηση για όλους τους εκθέτες που είναι μικρότεροι από k, τότε το ίδιο ισχύει και για τον εκθέτη k.

Λήμμα 2.3.1. *Έστω $k \geqslant 2$ και $0 \leqslant \ell \leqslant k$. Υπάρχουν θετικοί ακέραιοι $B_{0,\ell}, B_{1,\ell}, \ldots, B_{\ell-1,\ell}$ που εξαρτώνται μόνο από τους k και ℓ, τέτοιοι ώστε*

$$x^{2\ell}T^{k-\ell} + \sum_{i=0}^{\ell-1} B_{i,\ell}x^{2i}T^{k-i} = \sum(2k) = \sum(2k),$$

για όλους τους ακεραίους x και T που ικανοποιούν την

$$x^2 \leqslant T.$$

Απόδειξη. Ξεκινώντας από την ταυτότητα του Hilbert για εκθέτη $k + \ell$ με $r = 5$ παίρνουμε:

$$(x_1^2 + \cdots + x_5^2)^{k+\ell} = \sum_{i=1}^{M_\ell} a_i(b_{i,1}x_1 + \cdots + b_{i,5}x_5)^{2k+2\ell},$$

όπου οι ακέραιοι M_l και $b_{i,j}$ και οι θετικοί ρητοί αριθμοί a_i εξαρτώνται μόνο από τους k και ℓ. Έστω U ένας μη αρνητικός ακέραιος. Από το θεώρημα του Lagrange, μπορούμε να γράψουμε

$$U = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

για κάποιους μη αρνητικούς ακέραιους x_1, x_2, x_3, x_4. Έστω $x_5 = x$. Από τα παραπάνω έχουμε την πολυωνυμική ταυτότητα

$$(x^2 + U)^{k+\ell} = \sum_{i=1}^{M_\ell} a_i (b_i x + c_i)^{2k+2\ell}, \tag{2.3.1}$$

όπου οι αριθμοί M_ℓ, a_i και $b_i = b_{i,5}$ εξαρτώνται μόνο από τους k και ℓ, και οι ακέραιοι $c_i = b_{i,1}x_1 + \cdots + b_{i,4}x_4$ εξαρτώνται από τους k,l και U. Παρατηρούμε επίσης ότι $2\ell \leqslant k + \ell$ διότι $\ell \leqslant k$. Παραγωγίζοντας το πολυώνυμο του αριστερού μέλους της σχέσης (2.3.1) 2ℓ φορές παίρνουμε

$$\frac{d^{2\ell}}{dx^{2\ell}}\Big((x^2 + U)^{k+\ell}\Big) = \sum_{i=0}^{\ell} A_{i,l} x^{2i} (x^2 + U)^{k-i},$$

όπου οι $A_{i,\ell}$ είναι θετικοί ακέραιοι που εξαρτώνται μόνο από τους k και ℓ. Παραγωγίζοντας τώρα το πολυώνυμο στο δεξιό μέλος της (2.3.1) 2ℓ φορές παίρνουμε

$$\begin{aligned}
&\frac{d^{2\ell}}{dx^{2\ell}}\left(\sum_{i=1}^{M_\ell} a_i (b_i x + c_i)^{2k+2\ell}\right) \\
&= \sum_{i=1}^{M_\ell} (2k+1)(2k+2)\cdots(2k+2\ell) b_i^{2\ell} a_i (b_i x + c_i)^{2k} \\
&= \sum_{i=0}^{M_\ell} a_i' (b_i x + c_i)^{2k} \\
&= \sum_{i=0}^{M_\ell} a_i' y_i^{2k},
\end{aligned}$$

όπου $y_i = |b_i x + c_i|$ είναι ένας μη αρνητικός ακέραιος και ο

$$a_i' = (2k+1)(2k+2)\cdots(2k+2\ell) b_i^{2\ell} a_i$$

είναι μη αρνητικός ρητός αριθμός ο οποιός εξαρτάται μόνο από τους k και ℓ. Έπεται ότι, αν ο x και ο U είναι ακέραιοι με $U \geqslant 0$, τότε υπάρχουν μη αρνητικοί ακέραιοι $y_1, \ldots, y_{M_\ell}$ τέτοιοι ώστε

$$\sum_{i=0}^{\ell} A_{i,\ell} x^{2i} (x^2 + U)^{k-i} = \sum_{i=0}^{M_\ell} a_i' y_i^{2k}.$$

Θεωρούμε x και T μη αρνητικούς ακεραίους τέτοιους ώστε $x^2 \leqslant T$. Αφού ο $A_{\ell,\ell}$ είναι ένας θετικός ακέραιος αριθμός, προκύπτει ότι $x^2 \leqslant T \leqslant A_{\ell,\ell} T$ και συνεπώς

$$U = A_{\ell,\ell} T - x^2 \geqslant 0.$$

Με αυτή την επιλογή του U, έχουμε

$$\begin{aligned}\sum_{i=0}^{\ell} A_{i,\ell}x^{2i}(x^2+U)^{k-i} &= \sum_{i=0}^{\ell} A_{i,\ell}x^{2i}(A_{\ell,\ell}T)^{k-i}\\ &= \sum_{i=0}^{\ell} A_{i,\ell}A_{\ell,\ell}^{k-i}x^{2i}T^{k-i}\\ &= A_{\ell,\ell}^{k-\ell+1}\sum_{i=0}^{\ell} A_{i,\ell}A_{\ell,\ell}^{\ell-i-1}x^{2i}T^{k-i}\\ &= A_{\ell,\ell}^{k-\ell+1}\sum_{i=0}^{\ell} B_{i,\ell}x^{2i}T^{k-i},\end{aligned}$$

όπου $B_{\ell,\ell}=1$ και ο $B_{i,\ell}=A_{i,\ell}A_{\ell,\ell}^{\ell-i-1}$ είναι θετικός ακέραιος για $i=0,\dots,\ell-1$. Θέτοντας τέλος

$$a_i'' = \frac{a_i'}{A_{\ell,\ell}^{k-\ell+1}}$$

βλέπουμε ότι

$$\begin{aligned}x^{2\ell}T^{k-\ell}+\sum_{i=0}^{\ell-1}B_{\ell,\ell}x^{2i}T^{k-i} = \sum_{i=0}^{\ell}B_{i,\ell}x^{2i}T^{k-i} &= \frac{\sum_{i=0}^{\ell}A_{i,\ell}x^{2i}(x^2+U)^{k-i}}{A_{\ell,\ell}^{k-\ell+1}}\\ &= \frac{\sum_{i=1}^{M_\ell}a_i'y_i^{2k}}{A_{\ell,\ell}^{k-\ell+1}} = \sum_{i=1}^{M_\ell}a_i''y_i^{2k} = \sum(2k),\end{aligned}$$

και η απόδειξη του λήμματος ολοκληρώθηκε. □

Θεώρημα 2.3.2 (Hilbert-Waring)**.** *Το σύνολο των μη αρνητικών k-οστών δυνάμεων είναι βάση πεπερασμένης τάξης για κάθε θετικό ακέραιο k.*

Απόδειξη. Με επαγωγή ως προς k. Η περίπτωση $k=1$ είναι προφανής, και η περίπτωση $k=2$ είναι το Θεώρημα 1.1.1 του Lagrange. Έστω λοιπόν $k\geqslant 3$, και ας υποθέσουμε ότι το σύνολο των ℓ-οστών δυνάμεων είναι βάση πεπερασμένης τάξης για κάθε $\ell<k$. Από το Θεώρημα 2.2.11, το σύνολο των 2ℓ-οστών δυνάμεων είναι βάση πεπερασμένης τάξης για $\ell=1,2,\dots,k-1$. Έτσι, υπάρχει ένας ακέραιος r τέτοιος ώστε, για κάθε μη αρνητικό ακέραιο n και για $\ell=1,2,\dots,k-1$, η εξίσωση

$$n = x_1^{2\ell}+\cdots+x_r^{2\ell}$$

έχει λύση στους μη αρνητικούς ακεραίους $x_{1,\ell},\dots,x_{r,\ell}$. (Για παράδειγμα μπορούμε να θέσουμε $r=\max\{g(2\ell):\ell=1,2,\dots,k-1\}$.)

Έστω $T\geqslant 2$. Επιλέγουμε ακέραιους $C_1,\dots,C_{k-1}$ τέτοιους ώστε

$$0\leqslant C_\ell < T$$

για $\ell=1,2,\dots,k-1$. Υπάρχουν μη αρνητικοί ακέραιοι $x_{j,\ell}$ για $j=1,\dots,r$ και $\ell=1,\dots,k-1$ τέτοιοι ώστε

$$x_{1,\ell}^{2\ell}+\cdots+x_{r,\ell}^{2\ell} = C_{k-\ell}. \tag{2.3.2}$$

Τότε

$$x_{j,\ell}^2 \leqslant \sum_{j=1}^{r} x_{j,\ell}^{2i} \leqslant C_{k-\ell} < T$$

για $j = 1, \ldots, r$, $\ell = 1, \ldots, k-1$, και $i = 1, \ldots, \ell$. Από το Λήμμα 2.3.1, υπάρχουν θετικοί ακέραιοι $B_{i,\ell}$ που εξαρτώνται μόνο από τους k και ℓ ώστε να ισχύει

$$x_{j,\ell}^{2\ell} T^{k-\ell} + \sum_{i=0}^{\ell-1} B_{i,\ell} x_{j,\ell}^{2i} T^{k-i} = \sum(2k) = \sum(k). \tag{2.3.3}$$

Αθροίζοντας την (2.3.3) για $j = 1, \ldots, r$ και χρησιμοποιώντας την (2.3.2), έχουμε

$$\begin{aligned}
&C_{k-\ell} T^{k-\ell} + \sum_{i=0}^{\ell-1} B_{i,\ell} T^{k-i} \sum_{j=1}^{r} x_{j,\ell}^{2i} \\
&= C_{k-\ell} T^{k-\ell} + T^{k-\ell+1} \sum_{i=0}^{\ell-1} B_{i,\ell} T^{\ell-1-i} \sum_{j=1}^{r} x_{j,\ell}^{2i} \\
&= C_{k-\ell} T^{k-\ell} + D_{k-\ell+1} T^{k-\ell+1} \\
&= \sum(k),
\end{aligned}$$

όπου

$$D_{k-\ell+1} = \sum_{i=0}^{\ell-1} B_{i,\ell} T^{\ell-1-i} \sum_{j=1}^{r} x_{j,\ell}^{2i}$$

για $\ell = 1, \ldots, k-1$. Ο ακέραιος $D_{k-\ell+1}$ προσδιορίζεται πλήρως από τους k, ℓ, T και $C_{k-\ell}$ και είναι ανεξάρτητος του C_{k-i} για $i \neq \ell$. Έστω

$$B^* = \max\{B_{i,\ell} : \ell = 1, \ldots, k-1, i = 0, 1, \ldots, \ell-1\}.$$

Έπεται ότι

$$\begin{aligned}
0 &\leqslant C_{k-\ell} T^{k-\ell} + D_{k-\ell+1} T^{k-\ell+1} \\
&= C_{k-\ell} T^{k-\ell} + \sum_{i=0}^{\ell-1} B_{i,\ell} T^{k-i} \sum_{j=1}^{r} x_{j,\ell}^{2i} \\
&< B^* \Big(T^{k-\ell+1} + rT^k + \sum_{i=1}^{\ell-1} T^{k-i+1} \Big) \\
&= B^* \Big(rT^k + T^{k-\ell+1} \sum_{i=1}^{\ell-1} T^i \Big) \\
&< B^* \Big(rT^k + \frac{T^{k+1}}{T-1} \Big) \\
&\leqslant (r+2) B^* T^k,
\end{aligned}$$

όπου χρησιμοποιήθηκαν τα εξής:

$$C_{k-\ell} T^{k-\ell} < T T^{k-\ell} = T^{k-\ell+1} \leqslant B^* T^{k-\ell+1}$$

καθώς $C_{k-\ell} < T$ και $B^* \geqslant 1$,

$$\sum_{i=0}^{\ell-1} B_{i,\ell} T^{k-i} \sum_{j=1}^{r} x_{j,\ell}^{2i} = B_{0,\ell} T^k \sum_{j=1}^{r} 1 + \sum_{i=1}^{\ell-1} B_{i,\ell} T^{k-i} \sum_{j=1}^{r} x_{j,\ell}^{2i} \leqslant B^* r T^k + B^* \sum_{i=1}^{\ell-1} T^{k-i+1}$$

αφού $\sum_{j=1}^{r} x_{j,\ell}^{2i} < T$ και τέλος $T/(T-1) \leqslant 2$ όταν $T \geqslant 2$. Έστω

$$C_k = D_1 = 0.$$

Έχουμε

$$\sum_{\ell=1}^{k-1} (C_{k-\ell} T^{k-\ell} + D_{k-\ell+1} T^{k-\ell+1}) = \sum_{\ell=1}^{k} (C_\ell + D_\ell) T^\ell = \sum(k)$$

και

$$0 \leqslant \sum_{\ell=1}^{k} (C_\ell + D_\ell) T^\ell < (k-1)(r+2) B^* T^k = E^* T^k,$$

όπου ο ακέραιος

$$E^* = (k-1)(r+2)B^*$$

προσδιορίζεται από τον k και είναι ανεξάρτητος του T. Αν επιλέξουμε

$$T \geqslant E^*,$$

έπεται ότι

$$0 \leqslant \sum_{\ell=1}^{k} (C_\ell + D_\ell) T^\ell < E^* T < T^{k+1},$$

και έτσι ο $\sum_{\ell=1}^{k} (C_\ell + D_\ell) T^\ell$ μπορεί να γραφεί στην μορφή

$$\sum_{\ell=1}^{k} (C_\ell + D_\ell) T^\ell = E_1 T + \cdots + E_{k-1} T^{k-1} + E_k T^k, \tag{2.3.4}$$

με

$$0 \leqslant E_i < T$$

για $i = 1, \ldots, k-1$ και

$$0 \leqslant E_k < E^*.$$

Με αυτόν τον τρόπο δείξαμε ότι κάθε επιλογή μιας $(k-1)$-άδας $(C_1, \ldots, C_{k-1})$ ακεραίων από το $\{0, 1, \ldots, T-1\}$ προσδιορίζει μια άλλη $(k-1)$-άδα $(E_1, \ldots, E_{k-1})$ ακεραίων από το $\{0, 1, \ldots, T-1\}$. Θα αποδείξουμε ότι αυτή η απεικόνιση είναι $1-1$ και επί.

Αρκεί να αποδείξουμε ότι είναι επί. Προς τούτο, έστω $(E_1, \ldots, E_{k-1})$ μια $(k-1)$-άδα ακεραίων από το $\{0, 1, \ldots, T-1\}$. Υπάρχει ένας απλός αλγόριθμος που παράγει ακεραίους $C_1, C_2, \ldots, C_{k-1} \in \{0, 1, \ldots, T-1\}$ τέτοιους ώστε η (2.3.4) να ικανοποιείται για κάποιον μη αρνητικό ακέραιο $E_k < E^*$. Έστω $C_1 = E_1$ και $I_2 = 0$. Καθώς $D_1 = 0$, έχουμε

$$(C_1 + D_1) T = E_1 T + I_2 T^2.$$

Ο ακέραιος C_1 προσδιορίζει τον ακέραιο D_2. Επιλέγουμε στην συνέχεια $C_2 \in \{0, 1, \ldots, T-1\}$ τέτοιον ώστε

$$C_2 + D_2 + I_2 \equiv E_2 \bmod T.$$

Συνεπώς,

$$C_2 + D_2 + I_2 = E_2 + I_3 T$$

για κάποιον ακέραιο I_3, και

$$\sum_{\ell=1}^{2} (C_\ell + D_\ell) T^\ell = \sum_{\ell=1}^{2} E_\ell T^\ell + I_3 T^3.$$

Ακριβώς με τον ίδιο τρόπο ο ακέραιος C_2 προσδιορίζει τον D_3.

Όμοια επιλέγουμε $C_3 \in \{0, 1, \ldots, T-1\}$ τέτοιον ώστε

$$C_3 + D_3 + I_3 \equiv E_3 \bmod T$$

και τότε

$$C_3 + D_3 + I_3 = E_3 + I_4 T$$

για κάποιον ακέραιο I_4, και

$$\sum_{\ell=1}^{3} (C_\ell + D_\ell) T^\ell = \sum_{\ell=1}^{3} E_\ell T^\ell + I_4 T^4.$$

Έστω $2 \leqslant j \leqslant k-1$, και ας υποθέσουμε ότι έχουμε κατασκευάσει ακέραιους I_j και

$$C_1, \ldots . C_{j-1} \in \{0, 1, \ldots, T-1\}$$

τέτοιους ώστε

$$\sum_{\ell=1}^{j-1} (C_\ell + D_\ell) T^\ell = \sum_{\ell=1}^{j-1} E_\ell T^\ell + I_j T^j.$$

Υπάρχει ένας μοναδικός ακέραιος $C_j \in \{0, 1, \ldots, T-1\}$ τέτοιος ώστε

$$C_j + D_j + I_j \equiv E_j \bmod T.$$

Τότε,

$$C_j + D_j + I_j = E_j + I_{j+1} T$$

για κάποιον ακέραιο I_{j+1}, και

$$\sum_{\ell=1}^{j} (C_\ell + D_\ell) T^\ell = \sum_{\ell=1}^{j} E_\ell T^\ell + I_{j+1} T^{j+1}.$$

Συνεχίζοντας επαγωγικά, βλέπουμε ότι η διαδικασία αυτή παράγει μια μοναδική ακολουθία ακεραίων $C_1, C_2, \ldots, C_{k-1} \in \{0, 1, \ldots, T-1\}$ τέτοια ώστε

$$\sum_{\ell=1}^{k-1} (C_\ell + D_\ell) T^\ell = \sum_{\ell=1}^{k-1} E_\ell T^\ell + I_k T^k.$$

Αφού $C_k = 0$ και ο ακέραιος C_{k-1} προσδιορίζει τον D_k, προκύπτει ότι

$$0 \leqslant \sum_{\ell=1}^{k}(C_\ell + D_\ell)T^\ell = \sum_{\ell=1}^{k-1} E_\ell T^\ell + (D_k + I_k)T^k = \sum_{\ell=1}^{k} E_\ell T^\ell < E^* T^k,$$

όπου $D_k + I_k = E_k$. Καθώς

$$0 \leqslant \sum_{\ell=1}^{k-1} E_\ell T^\ell \leqslant \sum_{\ell=1}^{k-1}(T-1)T^\ell = T^k - T < T^k$$

και

$$0 \leqslant E_k < E^*,$$

προκύπτει ότι

$$\sum_{\ell=1}^{k-1} E_\ell T^\ell + E^* T^k < (1 + E^*)T^k \leqslant 2E^* T^k. \tag{2.3.5}$$

Προηγουμένως δείξαμε ότι

$$\sum_{\ell=1}^{k} E_\ell T^\ell = \sum_{\ell=1}^{k}(C_\ell + D_\ell)T^\ell = \sum(k).$$

Ο E^* εξαρτάται μόνο από τον k και όχι από τον T, και έτσι συμπεραίνουμε ότι

$$(E^* - E_k)T^k = \sum(k),$$

και συνεπώς,

$$\sum_{\ell=1}^{k-1} E_\ell T^\ell + E^* T^k = \sum_{\ell=1}^{k} E_\ell T^\ell + (E^* - E_k)T^k = \sum(k) + \sum(k) = \sum(k) \tag{2.3.6}$$

για κάθε $(k-1)$-άδα ακεραίων $(E_1, \ldots, E_{k-1})$ από το $\{0, 1, \ldots, T-1\}$. Καθώς η $\left(\frac{T+1}{T}\right)^k$ συγκλίνει στο 1 όταν το T τείνει στο άπειρο, μπορούμε να επιλέξουμε τον ακέραιο $T_0 > 5E^*$ έτσι ώστε

$$4(T+1)^k \leqslant 5T^k$$

για κάθε $T \geqslant T_0$. Θα δείξουμε ότι εάν $T \geqslant T_0$ και εάν $(F_0, F_1, \ldots, F_{k-1})$ είναι μια k-άδα ακεραίων στο $\{0, 1, \ldots, T-1\}$, τότε

$$F_0 + F_1 T + \cdots + F_{k-1}T^{k-1} + 4E^* T^k = \sum(k).$$

Θα χρησιμοποιήσουμε το ακόλουθο τέχνασμα. Έστω $E_0 \in \{0, 1, \ldots, T-1\}$. Εφαρμόζοντας την (2.3.5) με $T+1$ στη θέση του T, παίρνουμε

$$E_0(T+1) + E^*(T+1)^k < (T+1)^2 + E^*(T+1)^k \leqslant (1+E^*)(T+1)^k \leqslant 2E^*(T+1)^k. \tag{2.3.7}$$

Ακόμα, εφαρμόζοντας την (2.3.6) με τον $T+1$ στην θέση του T, έχουμε

$$E_0(T+1) + E^*(T+1)^k = \sum(k). \tag{2.3.8}$$

Προσθέτοντας τώρα τις (2.3.6) και (2.3.8), βλέπουμε ότι για κάθε επιλογή k το πλήθος ακεραίων

$$E_0, E_1, \dots, E_{k-1} \in \{0, 1, \dots, T-1\},$$

έχουμε

$$\begin{aligned} F^* &= \left(E_1 T + \cdots + E_{k-1}T^{k-1} + E^*T^k\right) + \left(E_0(T+1) + E^*(T+1)^k\right) \\ &= (E_0 + E^*) + (E_1 + E_0 + kE^*)T + \sum_{\ell=2}^{k-1}\left(E_\ell + \binom{k}{\ell}E^*\right)T^\ell + 2E^*T^k \\ &= \sum(k). \end{aligned}$$

Επιπλέον, από τις (2.3.5) και (2.3.7) προκύπτει ότι

$$0 \leqslant F^* < 2E^*T^k + 2E^*(T+1)^k < 4E^*(T+1)^k \leqslant 5E^*T^k < T^{k+1}$$

καθώς $4(T+1)^k \leqslant 5T^k$ και $T \geqslant T_0 > 5E^*$. Κατά συνέπεια, ο αριθμός F^* μπορεί να γραφτεί στη μορφή

$$F^* = F_0 + F_1 T + \cdots + F_{k-1}T^{k-1} + F_k T^k,$$

όπου $F_0, F_1, \dots, F_{k-1} \in \{0, 1, \dots, T-1\}$ και $F_k \leqslant 5E^*$. Με αυτόν τον τρόπο δείξαμε, όπως πριν, ότι εάν $T \geqslant T_0$ τότε κάθε επιλογή μιας k-άδας αριθμών $E_0, E_1, \dots, E_{k-1} \in \{0, 1, \dots, T-1\}$, προσδιορίζει μια άλλη k-άδα $(F_0, F_1 \dots, F_{k-1})$ ακεραίων από το $\{0, 1, \dots, T-1\}$. Θα δείξουμε ότι η απεικόνιση είναι 1-1 και επί. Αρκεί να δείξουμε ότι είναι επί. Έστω μια k-άδα ακεραίων $(F_0, F_1 \dots, F_{k-1}) \in \{0, 1, \dots, T-1\}$ Εφαρμόζοντας πάλι τον αλγόριθμο θα βρούμε ακεραίους F_k και

$$E_0, E_1, \dots, E_{k-1} \in \{0, 1, \dots, T-1\},$$

τέτοιους ώστε

$$\begin{aligned} &F_0 + F_1 T + \cdots + F_{k-1}T^{k-1} + F_k T^k \\ &= E_1 T + \cdots + E_{k-1}T^{k-1} + E^*T^k + E_0(T+1) + E^*(T+1)^k, \end{aligned}$$

όπου F_k είναι ένας ακέραιος που ικανοποιεί την ανισότητα

$$0 \leqslant F_k < 5E^*.$$

Θέτουμε $D_0 = E^*$, $D_\ell = \binom{k}{\ell}E^*$ για $\ell = 2, \dots, k-1$ και $D_k = 2E^*$. Επιλέγουμε $E_0 \in \{0, 1, \dots, T-1\}$ τέτοιον ώστε

$$E_0 + D_0 \equiv F_0 \bmod T.$$

Συνεπώς υπάρχει ακέραιος I_1 τέτοιος ώστε

$$E_0 + D_0 = F_0 + I_1 T.$$

Ορίζουμε $D_1 = E_0' + E^*$. Στη συνέχεια επιλέγουμε E_1 τέτοιον ώστε

$$E_1 + D_1 + I_1 \equiv F_1 \bmod T.$$

Άρα υπάρχει ακέραιος I_2 τέτοιος ώστε

$$E_1 + D_1 = F_1 - I_1 + I_2 T,$$

και έτσι έχουμε

$$\sum_{\ell=0}^{1} (E_\ell + D_i) T^\ell = F_0 + F_1 + I_2 T^2.$$

Συνεχίζοντας με αυτόν τον τρόπο βρίσκουμε τη ζητούμενη k-άδα αριθμών. Δείξαμε λοιπόν ότι για κάθε $T \geqslant T_0$ και κάθε $F_0, F_1, \ldots, F_{k-1} \in \{0, 1, \ldots, T-1\}$, $F_k \leqslant 5E^*$ ισχύει

$$F_0 + F_1 T + \cdots + F_k T^k = \sum(k).$$

Μετά και την πρόσθεση του $(5E^* - F_k)T^k = \sum(k)$, έχουμε ότι

$$F_0 + F_1 T + \cdots + F_{k-1} T^{k-1} + 5E^* T^k = \sum(k)$$

για όλα τα $T \geqslant T_0$ και για κάθε επιλογή $F_0, F_1, \ldots, F_{k-1} \in \{0, 1, \ldots, T-1\}$. Αυτό αποδεικνύει ότι $n = \sum(k)$ αν $T \geqslant T_0$ και

$$5E^* T^k \leqslant n < (5E^* + 1)T^k.$$

Υπάρχει ένας ακέραιος $T_1 \geqslant T_0$ με

$$5E^*(T+1)^k < (5E^* + 1)T^k$$

για κάθε $T \geqslant T_1$. Έτσι δείξαμε ότι $n = \sum(k)$ αν $T \geqslant T_1$ και

$$5E^* T^k \leqslant n < 5E^*(T+1)^k. \tag{2.3.9}$$

Καθώς κάθε ακέραιος $n \geqslant 5E^* T_1^k$ ικανοποιεί την ανισότητα (2.3.9) για κάποιον $T \geqslant T_1$, συμπεραίνουμε ότι

$$n = \sum(k)$$

για όλους τους n με $n \geqslant 5E^* T_1^k$. Το τελικό συμπέρασμα τώρα προκύπτει άμεσα από το Λήμμα 2.2.10. □

ΚΕΦΑΛΑΙΟ 3

Η ανισότητα του Weyl

3.1 Διοφαντική προσέγγιση

Σε αυτό το κεφάλαιο αναπτύσσουμε κάποια αναλυτικά εργαλεία τα οποία θα χρειαστούμε για την απόδειξη του ασυμπτωτικού τύπου των Hardy-Littlewood για το πρόβλημα του Waring. Τα πιο σημαντικά από αυτά τα εργαλεία είναι δύο ανισότητες για εκθετικά αθροίσματα, η ανισότητα του Weyl και το λήμμα του Hua. Θα χρειαστεί επίσης να θυμηθούμε την άθροιση κατά μέρη, τα απειρογινόμενα και τα γινόμενα Euler.

Αρχίζουμε με το ακόλουθο απλό αποτέλεσμα για την προσέγγιση πραγματικών αριθμών από ρητούς με μικρούς παρονομαστές. Συμβολίζουμε με $[x]$ το ακέραιο μέρος του πραγματικού αριθμού x και με $\{x\}$ το κλασματικό μέρος του x, δηλαδή $\{x\} = x - [x]$.

Θεώρημα 3.1.1 (Dirichlet). *Έστω α και $Q \geqslant 1$ πραγματικοί αριθμοί. Υπάρχουν ακέραιοι a και q τέτοιοι ώστε*

$$1 \leqslant q \leqslant Q, \qquad (a,q) = 1,$$

και

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

Απόδειξη. Έστω $N = [Q]$. Αν υποθέσουμε ότι $\{q\alpha\} \in [0, 1/(N+1))$ για κάποιον θετικό ακέραιο αριθμό $q \leqslant N$ τότε θέτοντας $a = [q\alpha]$ έχουμε ότι

$$0 \leqslant \{q\alpha\} = q\alpha - [q\alpha] = q\alpha - a < \frac{1}{N+1},$$

και έτσι

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q(N+1)} < \frac{1}{qQ} \leqslant \frac{1}{q^2}.$$

Ομοίως αν $\{q\alpha\} \in [N/(N+1), 1)$ για κάποιον θετικό ακέραιο αριθμό $q \leqslant N$ και αν $a = [q\alpha] + 1$, τότε καθώς

$$\frac{N}{N+1} \leqslant \{q\alpha\} = q\alpha - a + 1 < 1$$

εύκολα προκύπτει ότι

$$|q\alpha - a| \leqslant \frac{1}{N+1},$$

και έτσι

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q(N+1)} < \frac{1}{qQ} \leqslant \frac{1}{q^2}.$$

Αν τώρα

$$\{q\alpha\} \in \Big[\frac{1}{N+1}, \frac{N}{N+1}\Big)$$

για όλους τους $q \in [1, N]$, τότε καθένας από τους N το πλήθος πραγματικούς αριθμούς $\{q\alpha\}$ ανήκει σε ένα από τα $N-1$ το πλήθος διαστήματα

$$\Big[\frac{i}{N+1}, \frac{i+1}{N+1}\Big) \qquad i = 1, \ldots, N-1.$$

Από την Αρχή της Περιστεροφωλιάς, υπάρχουν ακέραιοι $i \in [1, N-1]$ και $q_1, q_2 \in [1, N]$ τέτοιοι ώστε

$$1 \leqslant q_1 < q_2 \leqslant N$$

και

$$\{q_1\alpha\}, \{q_2\alpha\} \in \Big[\frac{i}{N+1}, \frac{i+1}{N+1}\Big).$$

Θέτουμε

$$q = q_2 - q_1 \in [1, N-1]$$

και

$$a = [q_2\alpha] - [q_1\alpha].$$

Τότε έχουμε ότι

$$|q\alpha - a| = |(q_2\alpha - [q_2\alpha]) - (q_1\alpha - [q_1\alpha])| = |\{q_2\alpha\} - \{q_1\alpha\}| < \frac{1}{N+1} < \frac{1}{Q},$$

και η απόδειξη ολοκληρώθηκε. □

3.2 Τελεστές διαφορών

Ο *τελεστής διαφορών προς τα εμπρός* Δ_d είναι ο γραμμικός τελεστής που ορίζεται για μια συνάρτηση f από τον τύπο

$$\Delta_d(f)(x) = f(x+d) - f(x).$$

Για $\ell \geqslant 2$ ορίζουμε τον *τελεστή διαδοχικών διαφορών* $\Delta_{d_\ell, d_{\ell-1}, \ldots, d_1}$ μέσω της

$$\Delta_{d_\ell, d_{\ell-1}, \ldots, d_1} = \Delta_{d_\ell} \circ \Delta_{d_{\ell-1}, \ldots, d_1} = \Delta_{d_\ell} \circ \Delta_{d_{\ell-1}} \circ \cdots \circ \Delta_{d_1}.$$

Για παράδειγμα,

$$\begin{aligned}\Delta_{d_2, d_1}(f)(x) &= \Delta_{d_2}(\Delta_{d_1}(f))(x) \\ &= (\Delta_{d_1}(f))(x+d_2) - (\Delta_{d_1}(f))(x) \\ &= f(x+d_2+d_1) - f(x+d_2) - f(x+d_1) + f(x)\end{aligned}$$

και

$$\Delta_{d_3,d_2,d_1}(f)(x) = f(x+d_3+d_2+d_1) - f(x+d_3+d_2) - f(x+d_3+d_1) - f(x+d_2+d_1) \\ + f(x+d_3) + f(x+d_2) + f(x+d_1) - f(x).$$

Συμβολίζουμε με $\Delta^{(\ell)}$ τον τελεστή διαδοχικών διαφορών $\Delta_{1,1,\dots,1}$ με $d_i = 1$ για $i = 1, \dots, \ell$. Τότε,

$$\Delta^{(2)}(f)(x) = f(x+2) - 2f(x+1) + f(x)$$

και

$$\Delta^{(3)}(f)(x) = f(x+3) - 3f(x+2) + 3f(x+1) - f(x).$$

Λήμμα 3.2.1. *Έστω $\ell \geqslant 1$. Τότε,*

$$\Delta^{(\ell)}(f)(x) = \sum_{j=0}^{\ell} (-1)^{\ell-j} \binom{\ell}{j} f(x+j).$$

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στο ℓ. Αν το ζητούμενο ισχύει για τον ℓ, τότε έχουμε

$$\begin{aligned}
&\Delta^{(\ell+1)}(f)(x) = \Delta(\Delta^{(\ell)}(f))(x) \\
&= \Delta\Big(\sum_{j=0}^{\ell} (-1)^{\ell-j} \binom{\ell}{j} f(x+j) \Big) \\
&= \sum_{j=0}^{\ell} (-1)^{\ell-j} \binom{\ell}{j} \Delta(f)(x+j) \\
&= \sum_{j=0}^{\ell} (-1)^{\ell-j} \binom{\ell}{j} f(x+j+1) + \sum_{j=0}^{\ell} (-1)^{\ell+1-j} \binom{\ell}{j} f(x+j) \\
&= \sum_{j=1}^{\ell+1} (-1)^{\ell+1-j} \binom{\ell}{j-1} f(x+j) + \sum_{j=0}^{\ell} (-1)^{\ell+1-j} \binom{\ell}{j} f(x+j) \\
&= f(x+\ell+1) + \sum_{j=1}^{\ell} (-1)^{\ell+1-j} \left(\binom{\ell}{j-1} + \binom{\ell}{j} \right) f(x+j) + (-1)^{\ell+1} f(x) \\
&= \sum_{j=0}^{\ell+1} (-1)^{(\ell+1)-j} \binom{\ell+1}{j} f(x+j),
\end{aligned}$$

όπου στην τελευταία ισότητα χρησιμοποιήθηκε η γνωστή ταυτότητα $\binom{\ell+1}{j} = \binom{\ell}{j-1} + \binom{\ell}{j}$. □

Στο επόμενο λήμμα υπολογίζουμε το πολυώνυμο που προκύπτει αν εφαρμόσουμε κάποιον τελεστή διαδοχικών διαφορών στο μονώνυμο $f(x) = x^k$.

Λήμμα 3.2.2. *Έστω $k \geqslant 1$ και $1 \leqslant \ell \leqslant k$. Έστω $\Delta_{d_\ell,\dots,d_1}$ ένας τελεστής διαδοχικών διαφορών. Τότε,*

$$\Delta_{d_\ell,\dots,d_1}(x^k) = \sum_{\substack{j_1+\cdots+j_\ell+j=k \\ j\geqslant 0, j_1\geqslant 1,\dots,j_\ell\geqslant 1}} \frac{k!}{j!j_1!\cdots j_\ell!} d_1^{j_1} \cdots d_\ell^{j_\ell} x^j = d_1 \cdots d_\ell \, p_{k-\ell}(x),$$

όπου $p_{k-\ell}(x)$ είναι πολυώνυμο βαθμού $k-\ell$ με μεγιστοβάθμιο συντελεστή $k(k-1)\cdots(k-\ell+1)$. Αν οι $d_1, \dots, d_\ell$ είναι ακέραιοι, τότε το $p_{k-\ell}(x)$ έχει ακέραιους συντελεστές.

Απόδειξη. Με επαγωγή ως προς ℓ. Για $\ell = 1$ έχουμε

$$\begin{aligned}\Delta_{d_1}(x^k) &= (x+d_1)^k - x^k \\ &= \sum_{j=0}^{k} \binom{k}{j} d_1^{k-j} x^j - x^k \\ &= \sum_{j=0}^{k-1} \binom{k}{j} d_1^{k-j} x^j \\ &= \sum_{j=0}^{k-1} \frac{k!}{j!(k-j)!} d_1^{k-j} x^j \\ &= \sum_{\substack{j_1+j=k \\ j\geqslant 0, j_1\geqslant 1}} \frac{k!}{j!j_1!} d_1^{j_1} x^j.\end{aligned}$$

Έστω $1 \leqslant \ell \leqslant k-1$, και ας υποθέσουμε ότι ο ισχυρισμός αληθεύει για τον ℓ. Τότε

$$\begin{aligned}&\Delta_{d_{\ell+1},d_\ell,\ldots,d_1}(x^k) \\ &= \Delta_{d_{\ell+1}}\Big(\Delta_{d_\ell,\ldots,d_1}(x^k)\Big) \\ &= \sum_{\substack{j_1+\cdots+j_\ell+m=k \\ m\geqslant 0, j_1\geqslant 1,\ldots,j_\ell\geqslant 1}} \frac{k!}{m!j_1!\cdots j_\ell!} d_1^{j_1}\cdots d_\ell^{j_\ell} \Delta_{d_{\ell+1}}(x^m) \\ &= \sum_{\substack{j_1+\cdots+j_\ell+m=k \\ m\geqslant 0, j_1\geqslant 1,\ldots,j_\ell\geqslant 1}} \frac{k!}{m!j_1!\cdots j_\ell!} d_1^{j_1}\cdots d_\ell^{j_\ell} \sum_{\substack{j_{\ell+1}+j=m \\ j\geqslant 0, j_{\ell+1}\geqslant 1}} \frac{m!}{j!j_{\ell+1}!} d_{\ell+1}^{j_{\ell+1}} x^j \\ &= \sum_{\substack{j_1+\cdots+j_\ell+m=k \\ m\geqslant 0, j_1\geqslant 1,\ldots,j_\ell\geqslant 1}} \sum_{\substack{j_{\ell+1}+j=m \\ j\geqslant 0, j_{\ell+1}\geqslant 1}} \frac{k!}{j!j_1!\cdots j_\ell! j_{\ell+1}!} d_1^{j_1}\cdots d_\ell^{j_\ell} d_{\ell+1}^{j_{\ell+1}} x^j \\ &= \sum_{\substack{j_1+\cdots+j_\ell+j_{\ell+1}+j=k \\ j\geqslant 0, j_1,\ldots,j_\ell,j_{\ell+1}\geqslant 1}} \frac{k!}{j!j_1!\cdots j_\ell! j_{\ell+1}!} d_1^{j_1}\cdots d_\ell^{j_\ell} d_{\ell+1}^{j_{\ell+1}} x^j,\end{aligned}$$

όπου στη δεύτερη ισότητα χρησιμοποιήθηκε η γραμμικότητα του τελεστη Δ. Καθώς οι διωνυμικοί συντελεστές $\frac{k!}{j!j_1!\cdots j_\ell!}$ είναι ακέραιοι, προκύπτει ότι οι $d_1,\ldots,d_\ell$ είναι και αυτοί ακέραιοι αριθμοί και έτσι το πολυώνυμο $p_{k-\ell}(x)$ έχει ακέραιους συντελεστές. Τέλος είναι φανερό ότι ο βαθμός του είναι $k-\ell$ και ο μεγιστοβάθμιος συντελεστής του έιναι ο $\frac{k!}{(k-\ell)!} = k(k-1)\cdots(k-\ell+1)$. □

Λήμμα 3.2.3. *Έστω $k \geqslant 2$. Τότε,*

$$\Delta_{d_{k-1},\ldots,d_1}(x^k) = d_1\cdots d_{k-1}k!\Big(x + \frac{d_1+\cdots+d_{k-1}}{2}\Big).$$

Απόδειξη. Από το Λήμμα 3.2.2 έχουμε

$$\Delta_{d_{k-1},\cdots,d_1}(x^k) = \sum_{\substack{j_1+\cdots+j_{k-1}+j=k \\ j_i\geqslant 1\forall i, j\geqslant 0}} \frac{k!}{j!j_1!\cdots j_{k-1}!} d_1^{j_1}\cdots d_{k-1}^{j_{k-1}} x^j.$$

Για να ισχύει η σχέση $j_1 + \cdots + j_{k-1} + j = k$ με $j_1, \ldots, j_{k-1} \geqslant 1$ και $j \geqslant 0$ πρέπει είτε $j = j_1 = \cdots = j_{k-1} = 1$ είτε $j = 0, j_i = 2$ για κάποιο $i = 1, \ldots, k-1$ και $j_\ell = 1$ για κάθε $\ell \neq i$. Συνεπώς η παραπάνω σχεση ισοδύναμα γράφεται

$$\begin{aligned}\Delta_{d_{k-1},\cdots,d_1}(x^k) &= \frac{k!}{1!1!\cdots 1!}d_1d_2\cdots d_{k-1}x + \sum_{i=1}^{k-1}\frac{k!}{0!2!1!\cdots 1!}d_1\cdots d_i^2\cdots d_{k-1}\\ &= d_1d_2\cdots d_{k-1}k!\left(x + \frac{d_1+\cdots+d_{k-1}}{2}\right).\end{aligned}$$

□

Λήμμα 3.2.4. *Έστω $\ell \geqslant 1$ και $\Delta_{d_\ell,\ldots,d_1}$ ένας τελεστής διαδοχικών διαφορών. Έστω $f(x) = \alpha x^k + \cdots$ πολυώνυμο βαθμού k. Τότε,*

$$\Delta_{d_\ell,\ldots,d_1}(f)(x) = d_1\cdots d_\ell(k(k-1)\cdots(k-\ell+1)\alpha x^{k-\ell} + \cdots)$$

αν $1 \leqslant \ell \leqslant k$ και

$$\Delta_{d_\ell,\ldots,d_1}(f)(x) = 0$$

αν $\ell > k$. Ειδικότερα, αν $\ell = k-1$ και $d_1\cdots d_{k-1} \neq 0$, τότε το

$$\Delta_{d_\ell,\ldots,d_1}(f)(x) = d_1\cdots d_{k-1}k!\alpha x + \beta$$

είναι πολυώνυμο βαθμού 1.

Απόδειξη. Έστω $f(x) = \sum_{j=1}^k \alpha_j x^j$, όπου $\alpha_k = \alpha$. Καθώς ο τελεστής διαφορών είναι γραμμικός έχουμε

$$\Delta_{d_\ell,\ldots,d_1}(f)(x) = \sum_{j=0}^k \alpha_j \Delta_{d_\ell,\ldots,d_1}(x^j) = d_1\cdots d_\ell\left(\frac{k!}{(k-\ell)!}\alpha x^{k-\ell} + \cdots\right)$$

και η απόδειξη του λήμματος είναι πλήρης. □

Λήμμα 3.2.5. *Έστω $1 \leqslant \ell \leqslant k$. Αν*

$$-P \leqslant d_1, \ldots, d_\ell, x \leqslant P,$$

τότε

$$\Delta_{d_\ell,\ldots,d_1}(x^k) \ll P^k,$$

με την σταθερά να εξαρτάται μόνο από το k.

Απόδειξη. Από το Λήμμα 3.2.2 και καθώς $-P \leqslant d_1, \ldots, d_\ell, x \leqslant P$ εύκολα προκύπτει ότι

$$\begin{aligned}|\Delta_{d_\ell,\ldots,d_1}(x^k)| &\leqslant \sum_{\substack{j_1+\cdots+j_\ell+j=k\\ j\geqslant 0, j_1,\ldots,j_\ell\geqslant 1}} \frac{k!}{j!j_1!\cdots j_\ell!}P^{j_1+\cdots+j_\ell+j}\\ &\leqslant \sum_{\substack{j_1+\cdots+j_\ell+j=k\\ j,j_1,\ldots,j_\ell\geqslant 0}} \frac{k!}{j!j_1!\cdots j_\ell!}P^k\\ &= (\ell+1)^kP^k \leqslant (k+1)^kP^k.\end{aligned}$$

και έτσι η απόδειξη ολοκληρώθηκε. □

Μπορούμε τώρα να δώσουμε μια απλή εφαρμογή των τελεστών διαφορών. Το πρόβλημα του Waring ρωτάει αν κάθε μη αρνητικός ακέραιος γράφεται ως άθροισμα φραγμένων το πλήθος k-οστών δυνάμεων. Μπορούμε να θέσουμε το εξής παρόμοιο ερώτημα: Είναι σωστό ότι κάθε ακέραιος γράφεται ως άθροισμα ή διαφορά φραγμένων το πλήθος k-οστών δυνάμεων; Αν η απάντηση είναι καταφατική, τότε για κάθε k υπάρχει ελάχιστος ακέραιος $v(k)$ τέτοιος ώστε η εξίσωση

$$n = \pm x_1^k \pm x_2^k \pm \cdots \pm x_{v(k)}^k \tag{3.2.1}$$

να έχει ακέραιες λύσεις για κάθε ακέραιο n. Αυτό το πρόβλημα είναι γνωστό ως το *απλό πρόβλημα του Waring* και είναι πράγματι αρκετά ευκολότερο να αποδείξουμε την ύπαρξη του $v(k)$ από το να αποδείξουμε την ύπαρξη του $g(k)$. Παραμένει όμως ανοικτό πρόβλημα ο ακριβής υπολογισμός του $v(k)$ για κάθε $k \geqslant 3$.

Θεώρημα 3.2.6 (απλό θεώρημα Waring)**.** *Για κάθε $k \geqslant 2$ ο $v(k)$ υπάρχει, και*

$$v(k) \leqslant 2^{k-1} + \frac{k!}{2}.$$

Απόδειξη. Εφαρμόζοντας τον $(k-1)-$οστό τελεστή διαφορών στο πολυώνυμο $f(x) = x^k$ και χρησιμοποιώντας τα Λήμματα 3.2.1 και 3.2.3 έχουμε

$$\Delta^{(k-1)}(x^k) = k!x + m = \sum_{\ell=0}^{k-1} (-1)^{k-1-\ell} \binom{k-1}{\ell} (x+\ell)^k,$$

όπου $m = \frac{1+1+\cdots+1}{2} k! = \frac{k-1}{2} k! = (k-1)! \frac{k(k-1)}{2} = (k-1)! \binom{k}{2}$. Με αυτόν τον τρόπο βλέπουμε ότι κάθε ακέραιος της μορφής $k!x + m$ μπορεί να γραφτεί ως άθροισμα ή διαφορά το πολύ

$$\sum_{\ell=0}^{k-1} \binom{k-1}{\ell} = (1+1)^{k-1} = 2^{k-1}$$

k-οστών δυνάμεων ακεραίων. Τώρα, γνωρίζουμε ότι για κάθε ακέραιο n μπορούμε να βρούμε ακεραίους q και r τέτοιους ώστε

$$n - m = k!q + r,$$

όπου

$$-\frac{k!}{2} < r \leqslant \frac{k!}{2}.$$

Καθώς ο r είναι το άθροισμα ή η διαφορά ακριβώς $|r|$ k-οστών δυνάμεων 1^k, συμπεραίνουμε ότι ο n μπορεί να γραφτεί ως άθροισμα το πολύ $2^{k-1} + k!/2$ ακεραίων της μορφής $\pm x^k$. □

3.3 Κλασματικά μέρη

Συμβολίζουμε με $[\alpha]$ το ακέραιο μέρος του πραγματικού αριθμού α και με $\{\alpha\}$ το κλασματικό μέρος του α. Τότε, $[\alpha] \in \mathbb{Z}$, $\{\alpha\} \in [0,1)$, και

$$\alpha = [\alpha] + \{\alpha\}.$$

Η απόσταση του πραγματικού αριθμού α από τον πλησιέστερο ακέραιο ορίζεται ως εξής:

$$\|\alpha\| = \min\{|n-\alpha| : n \in \mathbb{Z}\} = \min\{\{\alpha\}, 1-\{\alpha\}\}.$$

Τότε, $\|\alpha\| \in [0, 1/2]$, και

$$\alpha = n \pm \|\alpha\|$$

για κάποιον ακέραιο n. Έπεται, κάνοντας χρήση των τριγωνομετρικών ταυτοτήτων

$$\sin(\alpha \pm \beta) = \sin\alpha\cos\beta \pm \sin\beta\cos\alpha,$$

ότι

$$|\sin\pi\alpha| = \sin\pi\|\alpha\|$$

για κάθε πραγματικό αριθμό α. Η τριγωνική ανισότητα

$$\|\alpha+\beta\| \leqslant \|\alpha\| + \|\beta\| \tag{3.3.1}$$

ισχύει για κάθε ζεύγος πραγματικών αριθμών α και β όπως αποδεικνύεται στην ακόλουθη πρόταση.

Πρόταση 3.3.1. *Για οποιουσδήποτε πραγματικούς αριθμούς α, β ισχύει η τριγωνική ανισότητα :*

$$\|\alpha+\beta\| \leqslant \|\alpha\| + \|\beta\|.$$

Απόδειξη. Παρατηρούμε ότι για κάθε πραγματικό αριθμό α έχουμε

$$\|x\| = \min(|n-x| : n \in \mathbb{Z}) = \min(\{x\}, 1-\{x\}) = \operatorname{dist}(x, \mathbb{Z}).$$

Έστω α, β πραγματικοί αριθμοί. Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι $0 \leqslant \alpha < 1$ και $0 \leqslant \beta < 1$ καθώς είναι προφανές ότι $\|x\| = \|n \pm x\|$ για κάθε πραγματικό αριθμό x και κάθε ακέραιο n.

Αν τουλάχιστον ένας εκ των α, β είναι μικρότερος από $1/2$, έστω χωρίς βλάβη ο α, έχουμε

$$\Big|\|\alpha+\beta\| - \|\beta\|\Big| = \big|\operatorname{dist}(\alpha+\beta, \mathbb{Z}) - \operatorname{dist}(\beta, \mathbb{Z})\big| \leqslant |\alpha| = \{\alpha\} = \|\alpha\|$$

καθώς η συνάρτηση $\operatorname{dist}(x, \mathbb{Z})$ είναι Lipschitz με σταθερά 1 και $0 \leqslant \alpha < 1/2$. Από αυτό έπεται το ζητούμενο.

Αν και οι δύο είναι μεγαλύτεροι από $1/2$ τότε οι αριθμοί $\gamma = 1-\alpha, \delta = 1-\beta$ είναι και οι δύο μικρότεροι του $1/2$. Εργαζόμαστε με τον ίδιο τρόπο και έχουμε

$$\|\alpha+\beta\| = \|2-(\alpha+\beta)\| = \|\gamma+\delta\| \leqslant \|\gamma\| + \|\delta\| = \|1-\alpha\| + \|1-\beta\| = \|\alpha\| + \|\beta\|,$$

και έτσι βλέπουμε ότι το ζητούμενο ισχύει σε κάθε περίπτωση. □

Τα δύο λήμματα που ακολουθούν είναι πολύ βασικά για την απόδειξη της ανισότητας του Weyl για εκθετικά αθροίσματα. Η ανισότητα του Weyl, με τη σειρά της, είναι το κεντρικό εργαλείο για την εφαρμογή της μεθόδου του κύκλου στο πρόβλημα του Waring. Σε ό,τι ακολουθεί, $\exp(t) = e^t$ και $e(t) = \exp(2\pi i t) = e^{2\pi i t}$.

Λήμμα 3.3.2. *Αν $0 < \alpha < 1/2$, τότε*

$$2\alpha < \sin(\pi\alpha) < \pi\alpha.$$

Απόδειξη. Θέτουμε $s(\alpha) = \sin(\pi\alpha) - 2\alpha$. Τότε $s(0) = s(1/2) = 0$. Αν $s(\alpha) = 0$ για κάποιον $\alpha \in (0, 1/2)$, τότε εφαρμόζοντας το θεώρημα του Rolle για την παραγωγίσιμη συνάρτηση s στα $[0, \alpha]$ και $[\alpha, 1/2]$, βλέπουμε ότι η συνάρτηση $s'(\alpha) = \pi\cos(\pi\alpha) - 2$ θα είχε τουλάχιστον δύο ρίζες στο διάστημα $(0, 1/2)$. Γνωρίζουμε όμως ότι η συνάρτηση $\cos(x)$ είναι γνησίως φθίνουσα στο διάστημα $(0, \pi/2)$ και συνεπώς η $s'(\alpha)$ είναι γνησίως φθίνουσα στο $(0, 1/2)$, το οποίο έρχεται σε αντίφαση με τα παραπάνω. Έτσι συμπεραίνουμε ότι $s(\alpha) \neq 0$ για κάθε $\alpha \in (0, 1/2)$. Καθώς τώρα η $s(\alpha)$ είναι συνεχής, διατηρεί πρόσημο στο $(0, 1/2)$. Υπολογίζουμε $s(1/4) = (\sqrt{2} - 1)/2 > 0$, και έτσι προκύπτει ότι $s(\alpha) > 0$ για κάθε $\alpha \in (0, 1/2)$. Το άνω φράγμα τώρα προκύπτει από την γνωστή ανισότητα $|\sin(x)| \leqslant |x|$ για κάθε $x \in \mathbb{R}$ με την ισότητα να ισχύει μόνο για $x = 0$. □

Λήμμα 3.3.3. *Για κάθε πραγματικό αριθμό α και για οποιουσδήποτε φυσικούς $N_1 < N_2$,*

$$\sum_{n=N_1+1}^{N_2} e(\alpha n) \leqslant \min\{N_2 - N_1, \|\alpha\|^{-1}\}.$$

Απόδειξη. Αφού $|e(\alpha n)| = 1$ για όλους τους ακεραίους n, έχουμε

$$\Big|\sum_{n=N_1+1}^{N_2} e(\alpha n)\Big| \leqslant \sum_{n=N_1+1}^{N_2} \Big|e(\alpha n)\Big| = N_2 - N_1.$$

Αν $\alpha \notin \mathbb{Z}$, τότε $\|\alpha\| > 0$ και $e(\alpha) \neq 1$. Αφού το άθροισμα είναι και γεωμετρική πρόοδος, έχουμε

$$\begin{aligned}
\Big|\sum_{n=N_1+1}^{N_2} e(\alpha n)\Big| &= \Big|e(\alpha(N_1+1)) \sum_{n=0}^{N_2-N_1+1} e(\alpha)^n\Big| = \Big|\frac{e(\alpha(N_2-N_1))-1}{e(\alpha)-1}\Big| \\
&\leqslant \frac{2}{|e(\alpha)-1|} = \frac{2}{|e(\alpha/2) - e(-\alpha/2)|} \\
&= \frac{2}{|2i\sin(\pi\alpha)|} = \frac{1}{|\sin(\pi\alpha)|} \\
&= \frac{1}{\sin(\pi\|\alpha\|)} \leqslant \frac{1}{2\|\alpha\|}.
\end{aligned}$$

Συνδυάζοντας τα δύο άνω φράγματα έχουμε τον ισχυρισμό του λήμματος. □

Λήμμα 3.3.4. *Έστω α πραγματικός αριθμός, και έστω a και $q \geqslant 1$ ακέραιοι με $(a, q) = 1$. Αν*

$$\Big|\alpha - \frac{a}{q}\Big| \leqslant \frac{1}{q^2},$$

τότε

$$\sum_{1 \leqslant r \leqslant q/2} \frac{1}{\|\alpha r\|} \ll q \log q.$$

Απόδειξη. Το λήμμα ισχύει για $q = 1$, καθώς

$$\sum_{1 \leqslant r \leqslant q/2} \frac{1}{\|\alpha r\|} = 0.$$

Συνεπώς, μπορούμε να υποθέσουμε ότι $q \geqslant 2$. Γνωρίζουμε ότι $\left\|\frac{ar}{q}\right\| \in \mathbb{Q}$ και $0 \leqslant \left\|\frac{ar}{q}\right\| \leqslant \frac{1}{2}$. Συνεπώς υπάρχουν ακέραιοι αριθμοί $s(r) \in [0, q/2]$ και $m(r)$ τέτοιοι ώστε

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

και έτσι προκύπτει ότι

$$\frac{ar}{q} = m(r) \pm \frac{s(r)}{q}$$

Καθώς $(a, q) = 1$ έχουμε

$$s(r) = 0 \iff \frac{s(r)}{q} = 0 \iff \left\|\frac{ar}{q}\right\| = 0 \iff \frac{ar}{q} \in \mathbb{Z} \iff q|ar \iff r|q \iff r \equiv 0 \bmod q,$$

και έτσι $s(r) \in [1, q/2]$ αν $r \in [1, q/2]$. Αφού $\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q^2}$ συμπεραίνουμε ότι υπάρχει πραγματικός αριθμός ϑ τέτοιος ώστε

$$\alpha - \frac{a}{q} = \frac{\vartheta}{q^2}$$

και $-1 \leqslant \vartheta \leqslant 1$. Έχουμε

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

όπου

$$|\vartheta'| = \left|\frac{2\vartheta r}{q}\right| \leqslant |\vartheta| \leqslant 1$$

αφού $\left|\frac{2r}{q}\right| \leqslant 1$. Τώρα προκύπτει ότι

$$\begin{aligned}
\|\alpha r\| &= \left\|\frac{ar}{q} + \frac{\vartheta'}{2q}\right\| \\
&= \left\|m(r) \pm \frac{s(r)}{q} + \frac{\vartheta'}{2q}\right\| \\
&= \left\|\frac{s(r)}{q} \pm \frac{\vartheta'}{2q}\right\| \\
&\geqslant \left\|\frac{s(r)}{q}\right\| - \left\|\frac{\vartheta'}{2q}\right\| \\
&\geqslant \frac{s(r)}{q} - \frac{1}{2q} \\
&\geqslant \frac{1}{q} - \frac{1}{2q} \\
&\geqslant \frac{1}{2q},
\end{aligned}$$

όπου στην πρώτη ανισότητα χρησιμοποιήσαμε την τριγωνική ανισότητα. Στη συνέχεια έστω $1 \leqslant r_1 \leqslant r_2 \leqslant q/2$. Θα αποδείξουμε ότι $s(r_1) = s(r_2)$ αν και μόνο αν $r_1 = r_2$. Προς τούτο έχουμε

$$s(r_1) = s(r_2) \iff \left\|\frac{ar_1}{q}\right\| = \left\|\frac{ar_2}{q}\right\| \iff \pm\left(\frac{ar_1}{q} - m(r_1)\right) = \pm\left(\frac{ar_2}{q} - m(r_2)\right)$$
$$\iff ar_1 \equiv \pm ar_2 \bmod q \Leftrightarrow r_1 \equiv \pm r_2 \bmod q.$$

όπου στην τελευταία ισοδυναμία χρησιμοποιήσαμε το ότι οι a και q είναι σχετικά πρώτοι μεταξύ τους αριθμοί. Αν $r_1 = r_2 \bmod q$ τότε καθώς $1 \leqslant r_1 \leqslant r_2 \leqslant q/2$ είναι φανερό ότι $r_1 = r_2$. Αν τώρα $r_1 = -r_2 \bmod q$ έχουμε $q|(r_1 + r_2)$ και εύκολα βλέπουμε ότι αυτό ισχύει μόνο αν $r_1 = r_2 = q/2$, και η απόδειξη του ισχυρισμού ολοκληρώθηκε.

Από τα παραπάνω έπεται ότι

$$\left\{\left\|\frac{ar}{q}\right\| : 1 \leqslant r \leqslant \frac{q}{2}\right\} = \left\{\frac{s(r)}{q} : 1 \leqslant r \leqslant \frac{q}{2}\right\} = \left\{\frac{s}{q} : 1 \leqslant s \leqslant \frac{q}{2}\right\},$$

και έτσι,

$$\begin{aligned}\sum_{1\leqslant r\leqslant q/2} \frac{1}{\|\alpha r\|} &\leqslant \sum_{1\leqslant r\leqslant q/2} \frac{1}{\frac{s(r)}{q} - \frac{1}{2q}} \\ &= \sum_{1\leqslant s\leqslant q/2} \frac{1}{\frac{s}{q} - \frac{1}{2q}} \\ &= 2q \sum_{1\leqslant s\leqslant q/2} \frac{1}{2s-1} \\ &\leqslant 2q \sum_{1\leqslant s\leqslant q/2} \frac{1}{s} \\ &\ll q\log q,\end{aligned}$$

και η απόδειξη ολοκληρώθηκε. □

Λήμμα 3.3.5. *Έστω α πραγματικός αριθμός και έστω a και $q \geqslant 1$ ακέραιοι με $(a,q) = 1$ και*

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q^2}.$$

Τότε, για κάθε μη αρνητικό πραγματικό αριθμό V και κάθε μη αρνητικό ακέραιο h, έχουμε

$$\sum_{r=1}^{q} \min\left\{V, \frac{1}{\|\alpha(hq+r)\|}\right\} \ll V + q\log q.$$

Απόδειξη. Έστω

$$\alpha = \frac{a}{q} + \frac{\vartheta}{q},$$

όπου

$$-1 \leqslant \vartheta \leqslant 1.$$

Τότε,

$$\begin{aligned}\alpha(hq+r) &= ah + \frac{ar}{q} + \frac{\vartheta h}{q} + \frac{\vartheta r}{q^2} \\ &= ah + \frac{ar}{q} + \frac{[\vartheta h] + \{\vartheta h\}}{q} + \frac{\vartheta r}{q^2} \\ &= ah + \frac{ar + [\vartheta h] + \delta(r)}{q},\end{aligned}$$

όπου $-1 \leqslant \delta(r) = \{\vartheta h\} + \frac{\vartheta r}{q} < 2$ καθώς $0 \leqslant \{\vartheta h\} < 1$ και $-1 \leqslant \frac{-r}{q} \leqslant \frac{\vartheta r}{q} \leqslant \frac{r}{q} \leqslant 1$. Για κάθε $r = 1, \ldots, q$ υπάρχει μοναδικός ακέραιος r' τέτοιος ώστε

$$\{\alpha(hq+r)\} = \frac{ar + [\vartheta h] + \delta(r)}{q} - r'.$$

Έστω

$$0 \leqslant t \leqslant 1 - \frac{1}{q}.$$

Αν

$$t \leqslant \{\alpha(hq+r)\} \leqslant t + \frac{1}{q},$$

τότε

$$qt \leqslant ar - qr' + [\vartheta h] + \delta(r) \leqslant qt + 1.$$

Από αυτό έπεται ότι

$$ar - qr' \leqslant qt - [\vartheta h] + 1 - \delta(r) \leqslant qt - [\vartheta h] + 2$$

και

$$ar - qr' \geqslant qt - [\vartheta h] - \delta(r) > qt - [\vartheta h] - 2.$$

Συνεπώς, ο $ar - qr'$ βρίσκεται στο ημιανοικτό διάστημα J μηκους 4, όπου

$$J = (qt - [\vartheta h] - 2, qt - [\vartheta h] + 2].$$

Αυτό το διάστημα περιέχει ακριβώς 4 διακεκριμένους ακεραίους. Αν $1 \leqslant r_1 \leqslant r_2 \leqslant q$ και

$$ar_1 - qr_1' = ar_2 - qr_2',$$

τότε

$$ar_1 \equiv ar_2 \bmod q$$

και καθώς $(a, q) = 1$ προκύπτει ότι

$$r_1 = r_2.$$

Έτσι, για κάθε $t \in [0, (q-1)/q]$, υπάρχουν 4 το πολύ ακέραιοι $r \in [1, q]$ τέτοιοι ώστε

$$\{\alpha(hq+r)\} \in [t, t + (1/q)].$$

Παρατηρούμε ότι

$$\|\alpha(hq+r)\| \in [t, t + (1/q)]$$

αν και μόνο αν

$$\{\alpha(hq+r)\} \in [t, t+(1/q)]$$

ή

$$1-\{\alpha(hq+r)\} \in [t, t+(1/q)].$$

Η τελευταία περίπτωση είναι ισοδύναμη με την

$$\{\alpha(hq+r)\} \in [t', t'+(1/q)],$$

όπου

$$0 \leqslant t' = 1 - \frac{1}{q} - t \leqslant 1 - \frac{1}{q}.$$

Έπεται ότι για κάθε $t \in [0, (q-1)/q]$, υπάρχουν το πολύ 8 ακέραιοι $r \in [1, q]$ με

$$\|\alpha(hq+r)\| \in [t, t+(1/q)].$$

Ειδικότερα, αν θέσουμε $J(s) = [s/q, (s+1)/q]$ για $s = 0, 1, \ldots$, έχουμε ότι

$$\|\alpha(hq+r)\| \in J(s)$$

για 8 το πολύ $r \in [1, q]$. Εφαρμόζουμε τώρα αυτό για να εκτιμήσουμε το άθροισμα

$$\sum_{r=1}^{q} \min\Big\{V, \frac{1}{\|\alpha(hq+r)\|}\Big\}.$$

Αν $\|\alpha(hq+r)\| \in J(0) = [0, 1/q]$, χρησιμοποιούμε την ανισότητα

$$\min\Big\{V, \frac{1}{\|\alpha(hq+r)\|}\Big\} \leqslant V.$$

Αν τώρα $\|\alpha(hq+r)\| \in J(s)$ για κάποιον $s \geqslant 1$, τότε χρησιμοποιούμε την ανισότητα

$$\min\Big\{V, \frac{1}{\|\alpha(hq+r)\|}\Big\} \leqslant \frac{1}{\|\alpha(hq+r)\|} \leqslant \frac{q}{s}.$$

Καθώς $\|\alpha(hq+r)\| \in J(s)$ μόνο για $s < q/2$, αφού $0 \leqslant \|\alpha(hq+r)\| \leqslant 1/2$, προκύπτει ότι

$$\sum_{r=1}^{q} \min\Big\{V, \frac{1}{\|\alpha(hq+r)\|}\Big\} \leqslant 8V + 8 \sum_{1 \leqslant s < q/2} \frac{q}{s} \ll V + q\log q,$$

το οποίο ολοκληρώνει την απόδειξη του λήμματος. □

Λήμμα 3.3.6. *Έστω α πραγματικός αριθμός, και έστω a και $q \geqslant 1$ ακέραιοι με $(a, q) = 1$ και*

$$\Big|\alpha - \frac{a}{q}\Big| \leqslant \frac{1}{q^2}.$$

Τότε, για κάθε πραγματικό αριθμό $U \geqslant 1$ και κάθε φυσικό n, έχουμε

$$\sum_{k=1}^{U} \min\Big\{\frac{n}{k}, \frac{1}{\|\alpha k\|}\Big\} \ll \Big(\frac{n}{q} + U + q\Big)\log(2qU).$$

Απόδειξη. Μπορούμε να γράψουμε τον k στη μορφή

$$k = hq + r,$$

όπου

$$1 \leqslant r \leqslant q$$

και

$$0 \leqslant h < \frac{U}{q}.$$

Τότε

$$S = \sum_{k=1}^{U} \min\Big\{\frac{n}{k}, \frac{1}{\|\alpha k\|}\Big\} \leqslant \sum_{0\leqslant h<U/q} \sum_{1\leqslant r\leqslant q} \min\Big\{\frac{n}{hq+r}, \frac{1}{\|\alpha(hq+r)\|}\Big\}.$$

Αν $h = 0$ και $1 \leqslant r \leqslant q/2$, τότε από το Λήμμα 3.3.4 προκύπτει

$$\sum_{r=1}^{q/2} \min\Big\{\frac{n}{r}, \frac{1}{\|\alpha r\|}\Big\} \leqslant \sum_{r=1}^{q/2} \frac{1}{\|\alpha r\|} \ll q \log q.$$

Για τους υπόλοιπους όρους, έχουμε

$$\frac{1}{hq+r} < \frac{2}{(h+1)q},$$

καθώς είτε $h \geqslant 1$ και

$$hq + r > hq \geqslant \frac{(h+1)q}{2},$$

είτε $h = 0, q/2 < r \leqslant q$, και

$$hq + r = r > \frac{q}{2} = \frac{(h+1)q}{2}.$$

Έτσι,

$$S \ll q \log q + \sum_{0\leqslant h<U/q} \sum_{1\leqslant r\leqslant q} \min\Big\{\frac{n}{(h+1)q}, \frac{1}{\|\alpha(hq+r)\|}\Big\}.$$

Παρατηρούμε ότι

$$\frac{U}{q} + 1 \leqslant U + q \leqslant 2\max\{q, U\} \leqslant 2qU.$$

Υπολογίζοντας το εσωτερικό άθροισμα από το Λήμμα 3.3.5 με $V = n/(h+1)q$, παίρνουμε

$$\begin{aligned}
S &\ll q \log q + \sum_{0\leqslant h<U/q} \sum_{1\leqslant r\leqslant q} \min\Big\{\frac{n}{(h+1)q}, \frac{1}{\|\alpha(hq+r)\|}\Big\} \\
&\ll q \log q + \sum_{0\leqslant h<U/q} \Big\{\frac{n}{(h+1)q} + q \log q\Big\} \\
&\ll q \log q + \frac{n}{q} \sum_{0\leqslant h<U/q} \frac{1}{h+1} + \Big(\frac{U}{q} + 1\Big) q \log q \\
&\ll q \log q + \frac{n}{q} \log\Big(\frac{U}{q} + 1\Big) + U \log q + q \log q \\
&\ll \Big(\frac{n}{q} + U + q\Big) \log(2qU),
\end{aligned}$$

και η απόδειξη ολοκληρώθηκε. □

Λήμμα 3.3.7. *Έστω α πραγματικός αριθμός, και έστω a και $q \geqslant 1$ ακέραιοι με $(a,q)=1$ και*

$$\Big|\alpha - \frac{a}{q}\Big| \leqslant \frac{1}{q^2}.$$

Τότε, για οποιουσδήποτε μη αρνητικούς πραγματικούς αριθμούς U και n, έχουμε

$$\sum_{k=1}^{U} \min\Big\{n, \frac{1}{\|\alpha k\|}\Big\} \ll \Big(q + U + n + \frac{Un}{q}\Big)\max\{1, \log q\}.$$

Απόδειξη. Το επιχείρημα που χρησιμοποιούμε είναι εντελώς ανάλογο με αυτό της απόδειξης του Λήμματος 3.3.6, δηλαδή γράφουμε τον k στην μορφή

$$k = hq + r,$$

όπου $0 \leqslant h < \frac{U}{q}$ και $1 \leqslant r \leqslant q$. Τώρα από το Λήμμα 3.3.5 έχουμε

$$\begin{aligned} S &= \sum_{1\leqslant k\leqslant U} \min\Big\{n, \frac{1}{\|\alpha k\|}\Big\} \\ &\leqslant \sum_{0\leqslant h<U/q} \sum_{1\leqslant r\leqslant q} \min\Big\{n, \frac{1}{\|\alpha(hq+r)\|}\Big\} \\ &\ll \sum_{0\leqslant h<U/q} (n + q\log q) \\ &\ll \Big(\frac{U}{q}+1\Big)(n+q\log q) \\ &\ll q\log q + U\log q + n + \frac{Un}{q} \\ &\ll \Big(q + U + n + \frac{Un}{q}\Big)\max\{1,\log q\}. \end{aligned}$$

Αυτό ολοκληρώνει την απόδειξη. □

3.4 Η ανισότητα του Weyl και το λήμμα του Hua

Σε ό,τι ακολουθεί, συμβολίζουμε με $[M,N]$ το διάστημα των ακεραίων m που ικανοποιούν την $M \leqslant m \leqslant N$. Για κάθε πραγματικό αριθμό t, ο μιγαδικός συζυγής του $e(t) = e^{2\pi i t}$ είναι ο $\overline{e(t)} = e(-t)$.

Λήμμα 3.4.1. *Έστω N_1, N_2 και N ακέραιοι τέτοιοι ώστε $N_1 < N_2$ και $0 \leqslant N_2 - N_1 \leqslant N$. Έστω $f(n)$ αριθμητική συνάρτηση με πραγματικές τιμές, και έστω*

$$S(f) = \sum_{n=N_1+1}^{N_2} e(f(n)).$$

Τότε,

$$|S(f)|^2 = \sum_{|d|<N} S_d(f),$$

όπου

$$S_d(f) = \sum_{n \in I(d)} e(\Delta_d(f)(n))$$

και $I(d)$ *είναι διάστημα διαδοχικών ακεραίων που περιέχεται στο* $[N_1+1, N_2]$.

Απόδειξη. Για κάθε ακέραιο d ορίζουμε

$$I(d) = [N_1 + 1 - d, N_2 - d] \cap [N_1 + 1, N_2].$$

Υψώνοντας την απόλυτη τιμή του εκθετικού αθροίσματος στο τετράγωνο παίρνουμε

$$\begin{aligned}
|S(f)|^2 = S(f)\overline{S(f)} &= \sum_{m=N_1+1}^{N_2} e(f(m)) \sum_{n=N_1+1}^{N_2} \overline{e(f(n))} \\
&= \sum_{n=N_1+1}^{N_2} \sum_{m=N_1+1}^{N_2} e(f(m) - f(n)) \\
&= \sum_{n=N_1+1}^{N_2} \sum_{d=N_1+1-n}^{N_2-n} e(f(n+d) - f(n)) \\
&= \sum_{n=N_1+1}^{N_2} \sum_{d=N_1+1-n}^{N_2-n} e(\Delta_d(f)(n)) \\
&= \sum_{d=-(N_2-N_1-1)}^{N_2-N_1-1} \sum_{n \in I(d)} e(\Delta_d(f)(n)) \\
&= \sum_{|d|<N} \sum_{n \in I(d)} e(\Delta_d(f)(n)) \\
&= \sum_{|d|<N} S_d(f).
\end{aligned}$$

Αυτός είναι ο ισχυρισμός του λήμματος. □

Λήμμα 3.4.2. *Έστω* N_1, N_2, N *και* ℓ *ακέραιοι τέτοιοι ώστε* $\ell \geqslant 1$ *και* $0 \leqslant N_2 - N_1 \leqslant N$. *Έστω* $f(n)$ *αριθμητική συνάρτηση με πραγματικές τιμές, και έστω*

$$S(f) = \sum_{n=N_1+1}^{N_2} e(f(n)).$$

Τότε,

$$|S(f)|^{2\ell} \leqslant (2N)^{2^\ell - \ell - 1} \sum_{|d_1|<N} \cdots \sum_{|d_\ell|<N} S_{d_\ell,\ldots,d_1}(f),$$

όπου

$$S_{d_\ell,\ldots,d_1}(f) = \sum_{n \in I(d_\ell,\ldots,d_1)} e(\Delta_{d_\ell,\ldots,d_1}(f)(n)) \tag{3.4.1}$$

και $I(d_\ell, \ldots, d_1)$ *είναι διάστημα διαδοχικών ακεραίων που περιέχεται στο* $[N_1+1, N_2]$.

Απόδειξη. Με επαγωγή ως προς ℓ. Η περίπτωση $\ell = 1$ είναι το Λήμμα 3.4.1. Υποθέτουμε ότι το αποτέλεσμα ισχύει για κάποιον $\ell \geqslant 1$. Χρησιμοποιώντας την ανισότητα Cauchy-Schwarz παίρνουμε

$$\begin{aligned}
|S(f)|^{2^{\ell+1}} &= \Big(|S(f)|^{2^\ell}\Big)^2 \\
&\leqslant \Big((2N)^{2^\ell-\ell-1} \sum_{|d_1|<N} \cdots \sum_{|d_\ell|<N} |S_{d_\ell,\ldots,d_1}(f)|\Big)^2 \\
&= (2N)^{2^{\ell+1}-2\ell-2}\Big(\sum_{|d_1|<N} \cdots \sum_{|d_\ell|<N} |S_{d_\ell,\ldots,d_1}(f)|\Big)^2 \\
&\leqslant (2N)^{2^{\ell+1}-2\ell-2}(2N)^\ell \sum_{|d_1|<N} \cdots \sum_{|d_\ell|<N} |S_{d_\ell,\ldots,d_1}(f)|^2,
\end{aligned}$$

όπου $S_{d_\ell,\ldots,d_1}(f)$ είναι ένα εκθετικό άθροισμα της μορφής (3.4.1). Εφαρμόζοντας το Λήμμα 3.4.1, για το $e(\Delta_{d_\ell,\ldots,d_1}(f)(n))$ στην θέση της f, έχουμε ότι για κάθε $d_1,\ldots,d_\ell$ υπάρχει κάποιο διάστημα

$$I(d_{\ell+1},d_\ell,\ldots,d_1) \subseteq I(d_\ell,\ldots,d_1) \subseteq [N_1+1,N_2]$$

τέτοιο ώστε

$$\begin{aligned}
|S_{d_\ell,\ldots,d_1}(f)|^2 &= \Big|\sum_{n\in I(d_1,\ldots,d_\ell)} e(\Delta_{d_\ell,\ldots,d_1}(f)(n))\Big|^2 \\
&= \sum_{|d_{\ell+1}|<N} \sum_{n\in I(d_{\ell+1},d_\ell,\ldots,d_1)} e(\Delta_{d_{\ell+1},d_\ell,\ldots,d_1}(f)(n)) \\
&= \sum_{|d_{\ell+1}|<N} S_{d_{\ell+1},d_\ell,\ldots,d_1}(f),
\end{aligned}$$

άρα

$$|S(f)|^{2^{\ell+1}} \leqslant (2N)^{2^{\ell+1}-(\ell+1)-1} \sum_{|d_1|<N} \cdots \sum_{|d_\ell|<N} \sum_{|d_{\ell+1}|<N} S_{d_{\ell+1},d_\ell,\ldots,d_1}(f).$$

Αυτό ολοκληρώνει την απόδειξη. □

Λήμμα 3.4.3. *Έστω $k \geqslant 1$, $K = 2^{k-1}$, και $\varepsilon > 0$. Έστω $f(x) = \alpha x^k + \cdots$ πολυώνυμο βαθμού k με πραγματικούς συντελεστές. Αν*

$$S(f) = \sum_{n=1}^{N} e(f(n)),$$

τότε

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

με την σταθερά να εξαρτάται μόνο από τους k και ε.

Απόδειξη. Εφαρμόζοντας το Λήμμα 3.4.2 με $\ell = k-1$ παίρνουμε

$$|S(f)|^K \leqslant (2N)^{K-k} \sum_{|d_1|<N} \cdots \sum_{|d_{k-1}|<N} |S_{d_{k-1},\ldots,d_1}(f)|,$$

όπου

$$S_{d_{k-1},\dots,d_1}(f) = \sum_{n\in I(d_{k-1},\dots,d_1)} e(\Delta_{d_{k-1},\dots,d_1}(f)(n))$$

και $I(d_{k-1},\dots,d_1)$ είναι ένα διάστημα ακεραίων που περιέχεται στο $[1,N]$. Αφού $|e(t)|=1$ για κάθε πραγματικό αριθμό t, έχουμε το άνω φράγμα

$$|S_{d_{k-1},\dots,d_1}(f)| \leqslant \sum_{n\in I(d_{k-1},\dots,d_1)} |e(\Delta_{d_{k-1},\dots,d_1}(f)(n))| = |I(d_{k-1},\dots,d_1)| \leqslant N.$$

Από το Λήμμα 3.2.4, για οποιουσδήποτε μη μηδενικούς ακεραίους $d_1,\dots,d_{k-1}$, ο τελεστής διαφορών $\Delta_{d_{k-1},\dots,d_1}$ εφαρμοσμένος στο πολυώνυμο $f(x)$ βαθμού k μας δίνει το γραμμικό πολυώνυμο

$$\Delta_{d_1,\dots,d_{k-1}}(f)(x) = d_{k-1}\cdots d_1 k!\alpha x + \beta = \lambda x + \beta,$$

όπου

$$\lambda = d_{k-1}\cdots d_1 k!\alpha$$

και $\beta\in\mathbb{R}$. Έστω $I(d_{k-1},\dots,d_1) = [N_1+1, N_2]$. Από το Λήμμα 3.3.3,

$$\begin{aligned}
|S_{d_{k-1},\dots,d_1}(f)| &= \Big|\sum_{n\in I(d_{k-1},\dots,d_1)} e(\Delta_{d_{k-1},d_{k-2},\dots,d_1}(f)(n))\Big| \\
&= \Big|\sum_{n=N_1+1}^{N_2} e(\lambda n+\beta)\Big| \\
&= \Big|\sum_{n=N_1+1}^{N_2} e(\lambda n)\Big| \\
&\leqslant \frac{1}{\|\lambda\|} \\
&= \frac{1}{\|d_{k-1}\cdots d_1 k!\alpha\|}.
\end{aligned}$$

Έπεται ότι

$$|S_{d_{k-1},\dots,d_1}(f)| \leqslant \min\{N, \|d_1\cdots d_{k-1}k!\alpha\|^{-1}\}.$$

Συνεπώς,

$$\begin{aligned}
|S(f)|^K &\leqslant (2N)^{K-k} \sum_{|d_1|<N} \cdots \sum_{|d_{k-1}|<N} |S_{d_{k-1},\dots,d_1}(f)| \\
&\leqslant (2N)^{K-k} \sum_{|d_1|<N} \cdots \sum_{|d_{k-1}|<N} \min\{N, \|d_1\cdots d_{k-1}k!\alpha\|^{-1}\}.
\end{aligned}$$

Υπάρχουν λιγότερες από $(k-1)(2N)^{k-2}$ επιλογές για τα $d_1,\dots,d_{k-1}$ τέτοιες ώστε $d_1\cdots d_{k-1}=0$,

και κάθε τέτοια επιλογή προσθέτει έναν όρο N στο άθροισμα, άρα

$$\begin{aligned}|S(f)|^K &\leqslant (2N)^{K-k}(k-1)(2N)^{k-2}N \\ &\quad + (2N)^{K-k}\sum_{1\leqslant|d_1|<N}\cdots\sum_{1\leqslant|d_{k-1}|<N}\min\{N,\|d_1\cdots d_{k-1}k!\alpha\|^{-1}\} \\ &\leqslant k(2N)^{K-1}+2^{k-1}N^{K-k}\sum_{1\leqslant d_1<N}\cdots\sum_{1\leqslant d_{k-1}<N}\min\{N,\|d_1\cdots d_{k-1}k!\alpha\|^{-1}\} \\ &\ll N^{K-1}+N^{K-k}\sum_{d_1=1}^{N}\cdots\sum_{d_{k-1}=1}^{N}\min\{N,\|d_1\cdots d_{k-1}k!\alpha\|^{-1}\},\end{aligned}$$

με τη σταθερά στην ανισότητα να εξαρτάται μόνο από το k. Αφού

$$1\leqslant d_1\cdots d_{k-1}k!\leqslant k!N^{k-1}$$

και η συνάρτηση του πλήθους διαιρετών $d(m)$, από το Θεώρημα Α.2.2, ικανοποιεί την $d(m)\ll_\varepsilon m^\varepsilon$ για κάθε $\varepsilon>0$, έπεται ότι το πλήθος των αναπαραστάσεων ενός ακεραίου m στη μορφή $d_1\cdots d_{k-1}k!$ είναι $\ll m^\varepsilon\ll N^\varepsilon$. Συνεπώς,

$$\begin{aligned}|S(f)|^K &\ll N^{K-1}+N^{K-k}\sum_{d_1=1}^{N}\cdots\sum_{d_{k-1}=1}^{N}\min\{N,\|d_{k-1}\cdots d_1k!\alpha\|^{-1}\} \\ &\ll N^{K-1}+N^{K-k+\varepsilon}\sum_{m=1}^{k!N^{k-1}}\min\{N,\|m\alpha\|^{-1}\},\end{aligned}$$

με τη σταθερά στην ανισότητα να εξαρτάται από τα k και ε. Έτσι, ολοκληρώνεται η απόδειξη. □

Θεώρημα 3.4.4 (ανισότητα του Weyl)**.** *Έστω $f(x)=\alpha x^k+\cdots$ πολυώνυμο βαθμού $k\geqslant 2$ με πραγματικούς συντελεστές. Υποθέτουμε ότι ο α έχει ρητή προσέγγιση a/q τέτοια ώστε*

$$\Big|\alpha-\frac{a}{q}\Big|\leqslant\frac{1}{q^2},$$

όπου $q\geqslant 1$ και $(a,q)=1$. Έστω

$$S(f)=\sum_{n=1}^{N}e(f(n)).$$

Έστω $K=2^{k-1}$ και $\varepsilon>0$. Τότε,

$$S(f)\ll N^{1+\varepsilon}\Big(\frac{1}{N}+\frac{1}{q}+\frac{q}{N^k}\Big)^{1/K},$$

με τη σταθερά να εξαρτάται μόνο από τους k και ε.

Απόδειξη. Αφού $|S(f)|\leqslant N$, το συμπέρασμα προκύπτει άμεσα αν $q\geqslant N^k$. Μπορούμε λοιπόν να υποθέσουμε ότι

$$1\leqslant q<N^k,$$

άρα

$$\log q\ll\log N\ll N^\varepsilon.$$

Από το Λήμμα 3.4.3 έχουμε

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

Από το Λήμμα 3.3.7 έχουμε

$$\begin{aligned}\sum_{m=1}^{k!N^{k-1}} \min\{N, \|m\alpha\|^{-1}\} &\ll \Big(q + k!N^{k-1} + N + \frac{k!N^k}{q}\Big) \max\{1, \log q\} \\ &\ll \Big(q + N^{k-1} + \frac{N^k}{q}\Big) \log N \\ &\ll N^k(qN^{-k} + N^{-1} + q^{-1})N^{\varepsilon}.\end{aligned}$$

Συνεπώς,

$$\begin{aligned}|S(f)|^K &\ll N^{K-1} + N^{K+\varepsilon}(qN^{-k} + N^{-1} + q^{-1}) \\ &\ll N^{K+\varepsilon}(qN^{-k} + N^{-1} + q^{-1}).\end{aligned}$$

Αυτό ολοκληρώνει την απόδειξη. □

Θεώρημα 3.4.5. *Έστω $k \geqslant 2$, και έστω a/q ρητός αριθμός με $q \geqslant 1$ και $(a, q) = 1$. Τότε,*

$$S(q, a) = \sum_{x=1}^{q} e(ax^k/q) \ll q^{1-\frac{1}{K}+\varepsilon}.$$

Απόδειξη. Εφαρμόζοντας την ανισότητα του Weyl με $f(x) = ax^k/q$ και $N = q$ παίρνουμε

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

που είναι το συμπέρασμα. □

Θεώρημα 3.4.6. *Έστω $k \geqslant 2$. Υπάρχει σταθερά $\delta > 0$ με την ακόλουθη ιδιότητα: Αν $N \geqslant 2$ και a/q είναι ρητός αριθμός τέτοιος ώστε $(a, q) = 1$ και*

$$N^{1/2} \leqslant q \leqslant N^{k-1/2},$$

τότε

$$\sum_{n=1}^{N} e(an^k/q) \ll N^{1-\delta}.$$

Απόδειξη. Εφαρμόζοντας την ανισότητα του Weyl για την $f(x) = ax^k/q$ παίρνουμε

$$\begin{aligned}S(f) &\ll N^{1+\varepsilon}(N^{-1} + q^{-1} + N^{-k}q)^{1/K} \leqslant N^{1+\varepsilon}(N^{-1} + N^{-1/2} + N^{-1/2})^{1/K} \\ &\leqslant N^{1-\frac{1}{2K}+\varepsilon} \leqslant N^{1-\delta}\end{aligned}$$

για κάθε $\delta < \frac{1}{2K}$. Αυτό ολοκληρώνει την απόδειξη. □

Θεώρημα 3.4.7 (το λήμμα του Hua). *Για $k \geqslant 2$ ορίζουμε*

$$T(\alpha) = \sum_{n=1}^{N} e(\alpha n^k).$$

Τότε,

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

Απόδειξη. Θα αποδείξουμε με επαγωγή ως προς j ότι

$$\int_0^1 |T(\alpha)|^{2^j} d\alpha \ll N^{2^j - j + \varepsilon}$$

για $j = 1, \ldots, k$. Η περίπτωση $j = 1$ προκύπτει άμεσα από την

$$\int_0^1 |T(\alpha)|^2 d\alpha = \sum_{m=1}^{N} \sum_{n=1}^{N} \int_0^1 e(\alpha(m^k - n^k))\, d\alpha = N.$$

Θεωρούμε $1 \leqslant j \leqslant k-1$ και υποθέτουμε ότι το αποτέλεσμα ισχύει για τον j. Έστω $f(x) = \alpha x^k$. Από το Λήμμα 3.2.2 έχουμε

$$\Delta_{d_j,\ldots,d_1}(f)(x) = \alpha d_j \cdots d_1 p_{k-j}(x),$$

όπου $p_{k-j}(x)$ είναι ένα πολυώνυμο βαθμού $k-j$ με ακέραιους συντελεστές. Εφαρμόζοντας το Λήμμα 3.4.2 με $N_1 = 0$, $N_2 = N$ και $S(f) = T(\alpha)$, παίρνουμε

$$\begin{aligned} |T(\alpha)|^{2^j} &\leqslant (2N)^{2^j - j + 1} \sum_{|d_1| < N} \cdots \sum_{|d_j| < N} \sum_{n \in I(d_j,\ldots,d_1)} e(\Delta_{d_j,\ldots,d_1}(f)(n)) \\ &= (2N)^{2^j - j + 1} \sum_{|d_1| < N} \cdots \sum_{|d_j| < N} \sum_{n \in I(d_j,\ldots,d_1)} e(\alpha d_j \cdots d_1 p_{k-j}(n)), \end{aligned}$$

όπου $I(d_j, \ldots, d_1)$ είναι ένα διάστημα διαδοχικών ακεραίων που περιέχεται στο $[1, N]$. Έπεται ότι

$$|T(\alpha)|^{2^j} \leqslant (2N)^{2^j - j + 1} \sum_{d} r(d) e(\alpha d), \tag{3.4.2}$$

όπου $r(d)$ είναι το πλήθος των παραγοντοποιήσεων του d στη μορφή

$$d = d_j \cdots d_1 p_{k-j}(n)$$

με $|d_i| \leqslant N$ και $n \in I(d_j, \ldots, d_1)$. Αφού $d \ll N^k$ από το Λήμμα Α.2.2 έχουμε

$$r(d) \ll |d|^{\frac{\varepsilon}{k}} \ll N^{\varepsilon}$$

για $d \neq 0$. Αφού το $p_{k-j}(x)$ είναι πολυώνυμο βαθμού $k - j \geqslant 1$, υπάρχουν το πολύ $k-j$ ακέραιοι x τέτοιοι ώστε $p_{k-j}(x) = 0$, άρα

$$r(0) \ll N^j.$$

Όμοια,

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

όπου $s(d)$ είναι το πλήθος των αναπαραστάσεων του d στη μορφή

$$d = \sum_{i=1}^{2^{j-1}} y_i^k - \sum_{i=1}^{2^{j-1}} x_i^k$$

με $1 \leqslant x_i, y_i \leqslant N$ για $i = 1, \dots, j-1$. Συνεπώς,

$$\sum_{d} s(d) = |T(0)|^{2^j} = N^{2^j}$$

και, από την επαγωγική υπόθεση,

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

Από την (3.4.2) έπεται ότι

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

και έχουμε αποδείξει το θεώρημα. □

ΚΕΦΑΛΑΙΟ 4

Ο ασυμπτωτικός τύπος των Hardy-Littlewood

4.1 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

$$r_{k,s}(N) = \mathfrak{G}(N)\Gamma\Big(1+\frac{1}{k}\Big)^s \Gamma\Big(\frac{s}{k}\Big)^{-1} N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\delta}), \tag{4.1.1}$$

όπου $\Gamma(x)$ είναι η συνάρτηση Γάμμα και $\mathfrak{G}(N)$ 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 (4.1.1) 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 στη 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 το ολοκλήρωμα 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 Waring, 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

$$P = [N^{1/k}].$$

Τότε,

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

και

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

4.2 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 4.2.1. *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. □

4.3 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

$$P = [N^{1/k}] \tag{4.3.1}$$

και

$$F(\alpha) = \sum_{m=1}^{P} e(\alpha m^k). \tag{4.3.2}$$

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

$$r_{k,s}(N) = \int_0^1 F(\alpha)^s e(-N\alpha)\, d\alpha. \tag{4.3.3}$$

Δεν μπορούμε να υπολογίσουμε αυτό το ολοκλήρωμα ακριβώς μέσω στοιχειωδών συναρτήσεων. Εντας 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* $\mathfrak{M}$ και τα *ελλάσσονα τόξα* $\mathfrak{m}$, 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» $\mathfrak{G}(N)$. 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, $P = [N^{1/k}] \geqslant 2$. Επιλέγουμε

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

Για

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

θέτουμε

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

και

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

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

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

και

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

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 $\alpha \in \mathfrak{M}(q,a) \cap \mathfrak{M}(q',a')$ 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 $\mathfrak{M}(q,a)$ είναι ξένα ανά δύο.

Το μέτρο του συνόλου $\mathfrak{M}(1,0) \cup \mathfrak{M}(1,1)$ είναι $2P^{\nu-k}$, και, για κάθε $q \geqslant 2$ με $(a,q) = 1$, το μέτρο του μείζονος τόξου $\mathfrak{M}(q,a)$ 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 $\mathfrak{M}$ των μειζόνων τόξων είναι

$$\mu(\mathfrak{M}) = \frac{2}{P^{k-\nu}} \sum_{1 \leqslant q \leqslant P^\nu} \varphi(q) \leqslant \frac{2}{P^{k-\nu}} \sum_{1 \leqslant q \leqslant P^\nu} q \leqslant \frac{2}{P^{k-\nu}} \frac{P^\nu(P^\nu+1)}{2} \leqslant \frac{2}{P^{k-3\nu}}, \tag{4.3.4}$$

που τείνει στο 0 όταν το P τείνει στο άπειρο.

Το σύνολο

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

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

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

Αν και το μέτρο του συνόλου $\mathfrak{m}$ 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 $r_{k,s}(N)$.

4.4 Τα ελάσσονα τόξα

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

Θεώρημα 4.4.1. *Έστω $k \geqslant 2$ και $s \geqslant 2^k + 1$. Υπάρχει $\delta_1 > 0$ τέτοιος ώστε*

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

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

Απόδειξη. Εφαρμόζοντας το Θεώρημα 3.1.1 (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 $\alpha \in \mathfrak{m}$, τότε $\alpha \notin \mathfrak{M}(1,0) \cup \mathfrak{M}(1,1)$, άρα

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

Επίσης, από την αρχική ανισότητα έπεται ότι

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

και συνεπώς

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

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

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

το οποίο είναι άτοπο. Συνεπώς,

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

Θέτουμε

$$K = 2^{k-1}. \tag{4.4.1}$$

Από την ανισότητα του Weyl (Θεώρημα 3.4.4) 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 3.4.7) παίρνουμε

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

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. □

4.5 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 $\mathfrak{M}(q,a)$ 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 3.4.5) έχουμε

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

άρα

$$\frac{S(q,a)}{q} \ll q^{-\frac{1}{K}+\varepsilon}, \tag{4.5.1}$$

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

Λήμμα 4.5.1. *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 $[1,\infty)$. Έπεται ότι

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

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 $M = [|\beta|^{-1}]$. Τότε,

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

Ορίζουμε $U(t) = \sum_{m \leqslant t} e(\beta m)$. Από το Λήμμα 3.3.3 έχουμε $U(t) \leqslant \|\beta\|^{-1} = |\beta|^{-1}$. Αθροίζοντας κατά μέρη (Θεώρημα Α.1.1) 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,

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

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 τη 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

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

Αυτό αποδεικνύει το λήμμα. □

Λήμμα 4.5.2. *Έστω q και α ακέραιοι τέτοιοι ώστε $1 \leqslant q \leqslant P^\nu$, $0 \leqslant \alpha \leqslant q$, και $(a,q)=1$. Αν $\alpha \in \mathfrak{M}(q,a)$, 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 $\alpha \in \mathfrak{M}(q,a)$, 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 $m = sq + r$ για d, r ακεραίους, έπεται ότι

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

καθώς

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

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

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

Έστω $t \geqslant 1$. Από τη μονοτονία της f έχουμε

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

άρα

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

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 4.5.3. *Εστω*

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

και

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

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

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

όπου $\delta_2 = (1-5\nu) > 0$.

Απόδειξη. Έστω $\alpha \in \mathfrak{M}(q,a)$ 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 4.5.1. Θέτουμε $F = F(\alpha)$. Τότε, $|F| \leqslant P$. Αφού $F - V = O(P^{2\nu})$ από το Λήμμα 4.5.2, 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 $\mu(\mathfrak{M}) \ll P^{3\nu-k}$ από την (4.3.4), έπεται ότι

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

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

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

Για $q \geqslant 2$ έχουμε

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

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

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

Συνεπώς,

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

και έχουμε το θεώρημα. □

4.6 Το ιδιάζον ολοκλήρωμα

Στη συνέχεια θεωρούμε το ολοκλήρωμα

$$J(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta N)\, d\beta. \tag{4.6.1}$$

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

Θεώρημα 4.6.1. *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 $g(\beta) = \min\{P, |\beta|^{-1/k}\}^s \geqslant 0$ 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 4.5.1 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 4.6.2. *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 εύκολο 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

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

και

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

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

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

και

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

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 4.6.3. *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 4.6.2 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 4.6.2 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. □

4.7 Η ιδιάζουσα σειρά και το θεώρημα των Hardy και Littlewood

Στο Θεώρημα 4.5.3 ορίσαμε την συνάρτηση

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

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

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

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 (4.5.1) βλέπουμε ότι

$$A_N(q) \ll \frac{q}{q^{\frac{s}{K}-s\varepsilon}} \leqslant \frac{1}{q^{1+\delta_4}}, \tag{4.7.1}$$

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

$$|\mathfrak{G}(N)| < c_2 \tag{4.7.2}$$

για όλους τους φυσικούς N. Επιπλέον,

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

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

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

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 4.7.1. *Έστω $(q, r) = 1$. Τότε κάθε κλάση ισοτιμίας* mod 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 mod 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

$$xr + yq \equiv x'r + y'q \bmod qr$$

και άρα

$$(x - x')r \equiv (y - y')q \bmod qr.$$

Από την σχέση αυτή πολλαπλασιάζοντας με r προκύπτει ότι

$$(x - x')r^2 \equiv (y - y')qr \bmod qr$$

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 4.7.2. *Έστω $(q, r) = 1$. Τότε κάθε αντιστρέψιμη κλάση ισοτιμίας* mod 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 mod 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 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 συνάρτηση φ του Euler είναι πολλαπλασιαστική. Όμοια με το προηγούμενο λήμμα, η g είναι $1-1$ άρα και επί. Η απόδειξη ολοκληρώθηκε. □

Λήμμα 4.7.3. *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 4.7.4. *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 4.7.3 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

$$x_1^k + \cdots + x_s^k \equiv N \bmod q$$

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

Λήμμα 4.7.5. *Έστω $s \geqslant 2^k + 1$. Για κάθε πρώτο p, η σειρά*

$$\chi_N(p) = 1 + \sum_{h=1}^{\infty} A_N(p^h) \tag{4.7.3}$$

συγκλίνει, και

$$\chi_N(p) = \lim_{h\to\infty} \frac{M_N(p^h)}{p^{h(s-1)}}. \tag{4.7.4}$$

Απόδειξη. Η σύγκλιση της σειράς (4.7.3) είναι άμεση συνέπεια της ανισότητας (4.7.1). 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 $m \equiv 0 \bmod q$ 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 $m \equiv 0 \bmod q$ και ίσο με 0 αλλιώς. Συνεπώς, 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 $x_1^k + \cdots + x_s^k \equiv N \bmod q$ 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 4.7.6. *Αν $s \geqslant 2^k + 1$, τότε*

$$\mathfrak{G}(N) = \prod_p \chi_N(p). \tag{4.7.5}$$

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

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

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

$$\frac{1}{2} \leqslant \prod_{p > p_0} \chi_N(p) \leqslant \frac{3}{2} \tag{4.7.6}$$

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 Θεώρημα Α.3.3 γνωρίζουμε ότι

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

και άρα και το γινόμενο Euler (4.7.5) συγκλίνει. Ειδικότερα, $\chi_N(p) \neq 0$ για κάθε N και p. Αφού ο $\chi_N(p)$ είναι μη αρνητικός από την (4.7.4), συμπεραίνουμε ότι ο $\chi_N(p)$ είναι θετικός πραγματικός αριθμός για κάθε N και p, συνεπώς η ιδιάζουσα σειρά $\mathfrak{G}(N)$ είναι θετική. Πάλι, από την (4.7.1),

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

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 Α.3.1, 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 (4.7.6). □

Θέλουμε να δείξουμε ότι ο $\mathfrak{G}(N)$ είναι φραγμένος μακρυά από το 0 ομοιόμορφα ως προς N. Από την ανισότητα (4.7.6), αρκεί να δείξουμε, για κάθε πρώτο p, ότι ο $\chi_N(p)$ είναι ομοιόμορφα φραγμένος μακριά από το 0.

Έστω p πρώτος, και έστω

$$k=p^rk_0,$$

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

Λήμμα 4.7.7. *Έστω m φυσικός που δεν διαιρείται από τον p. Αν η ισοτιμία $x^k\equiv m \bmod p^\gamma$ έχει λύση, τότε η ισοτιμία $y^k\equiv m \bmod p^h$ 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 $\bmod p^h$ 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 $\bmod p^h$. Τότε, ο g είναι επίσης πρωταρχική ρίζα $\bmod p^\gamma$. Έστω $x^k\equiv m \bmod p^\gamma$. Τότε $(x,p)=1$, και μπορούμε να επιλέξουμε ακεραίους r και u τέτοιους ώστε

$$x\equiv g^u \bmod p^h$$

και

$$m\equiv g^r \bmod p^h.$$

Συνεπώς έχουμε

$$g^{ku}-g^r\equiv g^r(g^{ku-r}-1)\equiv 0 \bmod p^h$$

και καθώς $(g,p)=1$, συμπεραίνουμε ότι

$$g^{ku-r}\equiv 1 \bmod p^h.$$

Αφού η τάξη του στοιχείου g είναι $\varphi(p^h) = p^{h-\gamma}\varphi(p^\gamma)$, προκύπτει ότι

$$ku \equiv r \bmod \varphi(p^\gamma),$$

άρα

$$r \equiv 0 \bmod (k, \varphi(p^\gamma))$$

και

$$r \equiv 0 \bmod (k, \varphi(p^h)).$$

Υπάρχει δηλαδή ακέραιος μ με

$$r = \mu(k, \varphi(p^h))$$

Θεωρούμε ακέραιους a, b τέτοιους ώστε

$$ak + b\varphi(p^h) = (k, \varphi(p^h))$$

και από τα παραπάνω έχουμε

$$r = ka\mu + b\varphi(p^h)\mu.$$

Θέτουμε $v = a\mu$ και έπεται

$$kv \equiv r \bmod \varphi(p^h).$$

Έστω $y = g^v$. Τότε,

$$y^k \equiv m \bmod p^h,$$

καθώς $g^{\varphi(p^h)} \equiv 1 \bmod p^h$.

Στη δεύτερη περίπτωση, έχουμε $p = 2$ άρα οι m και x είναι περιττοί. Αν $r = 0$ τότε ο k είναι περιττός. Έστω y_1,y_2 δύο περιττές κλάσεις υπολοίπων $\bmod 2^h$. Τότε αν

$$y_1^k \equiv y_2^k \bmod 2^h,$$

έπεται ότι ο 2^h διαιρεί τον αριθμό $y_1^k - y_2^k = (y_1 - y_2)(y_1^{k-1} + y_1^{k-2}y_2 + \cdots + y_2^{k-1})$, και καθώς ο $y_1^{k-1} + y_1^{k-2}y_2 + \cdots + y_2^{k-1}$ είναι περιττός έχουμε

$$y_1 \equiv y_2 \bmod 2^h.$$

Καθώς λοιπόν ο y διατρέχει το σύνολο των περιττών κλάσεων ισοτιμίας $\bmod 2^h$, το ίδιο ισχύει για τον y^k, και η ισοτιμία $y^k \equiv m \bmod 2^h$ έχει λύση για κάθε $h \geqslant 1$. Αν $r \geqslant 1$ τότε ο k είναι άρτιος και $m \equiv x^k \equiv 1 \bmod 4$. Επίσης, $x^k = (-x)^k$, άρα μπορούμε να υποθέσουμε ότι $x \equiv 1 \bmod 4$. Οι κλάσεις ισοτιμίας $\bmod 2^h$ 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

$$m \equiv 5^r \bmod 2^h$$

και

$$x \equiv 5^u \bmod 2^h.$$

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

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

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

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

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

Λήμμα 4.7.8. *Έστω p πρώτος. Αν υπάρχουν ακέραιοι $a_1, \ldots, a_s$, που δεν διαιρούνται όλοι από τον p, τέτοιοι ώστε*

$$a_1^k + \cdots + a_s^k \equiv N \bmod p^\gamma,$$

τότε

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

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

$$x_i \equiv a_i \bmod p^\gamma.$$

Αφού η ισοτιμία

$$x_1^k \equiv N - x_1^k - \cdots - x_s^k \bmod p^\gamma$$

έχει λύση $x_1 = a_1 \not\equiv 0 \bmod p$, από το Λήμμα 4.7.7 βλέπουμε ότι η

$$x_1^k \equiv N - x_1^k - \cdots - x_s^k \bmod p^h$$

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 4.7.9. *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 4.7.8 αρκεί να αποδείξουμε ότι η ισοτιμία

$$a_1^k + \cdots + a_s^k \equiv N \bmod p^\gamma \tag{4.7.7}$$

έχει λύση στους ακεραίους a_i με τουλάχιστον έναν από τους a_i να μην διαιρείται από τον p. Αν ο N δεν διαιρείται από τον p και η ισοτιμία έχει λύση, τότε τουλάχιστον ένας από τους ακεραίους a_i δεν διαιρείται από τον p. Αν $N \equiv 0 \bmod p$, αρκεί να δείξουμε ότι η ισοτιμία

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

έχει λύση. Ισοδύναμα, αρκεί να λύσουμε την ισοτιμία

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

Σε αυτήν την περίπτωση έχουμε $(N-1,p)=1$. Αρκεί λοιπόν να δείξουμε ότι αν $(N,p)=1$ τότε η ισοτιμία (4.7.7) 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

$$x^k \equiv m \bmod p^\gamma.$$

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

$$kv \equiv r \bmod (p-1)p^r.$$

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

$$r \equiv 0 \bmod (k_0, p-1)p^r,$$

και συνεπώς 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 (4.7.7) 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-οστών δυνάμεων $\bmod p^\gamma$. Έστω $(m,p)=1$ και $N' = m^k N$. Αν

$$a_1^k + \cdots + a_s^k \equiv N \bmod p^\gamma,$$

τότε έχουμε

$$(ma_1)^k + \cdots + (ma_s)^k \equiv m^k N \bmod p^\gamma,$$

συνεπώς $s(N') \leqslant s(N)$. Έστω τώρα $a_1, a_2, \ldots, a_s$ τέτοιοι ώστε

$$a_1^k + \cdots + a_s^k \equiv m^k N \bmod p^\gamma.$$

Αφού $(m,p^\gamma)=1$, υπάρχουν ακέραιοι x,y τέτοιοι ώστε

$$xm + yp^\gamma = 1.$$

Έτσι, για κάθε $i = 1,2,\ldots,s$ υπάρχει ακέραιος λ_i με

$$(a_i xm + a_i y p^\gamma)^k = (a_i x)^k m^k + \lambda_i p^\gamma \equiv a_i^k \bmod p^\gamma.$$

Θέτοντας $b_i = a_i x$, έχουμε

$$(b_1^k + \cdots + b_s^k)m^k \equiv m^k N \bmod p^\gamma$$

και καθώς (m,p^γ) προκύπτει ότι

$$b_1^k + \cdots + b_s^k \equiv N \bmod p^\gamma,$$

δηλαδη $s(N) \leqslant s(N')$. Συνεπώς $s(N') = s(N)$. 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 $i = 1$ και 2. Ακόμα από την ελαχιστικότητα του N προκύπτει ότι $s(N-i) \leqslant j$. Αφού $N = (N-1)+1^k$ και $N = (N-2)+1^k+1^k$, έπεται ότι

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

άρα $s(N-i) = j$ ή $j-1$. Αυτό σημαίνει ότι δεν υπάρχουν διαδοχικά μη κενά σύνολα $C(j)$ 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

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

Έτσι συμπεραίνουμε ότι $s(N) \leqslant 2k-1$ αν ο p είναι 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 (4.7.7) 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 4.7.10. *Υπάρχουν θετικές σταθερές $c_1 = c_1(k,s)$ και $c_2 = c_2(k,s)$ τέτοιες ώστε*

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

Επιπλέον, για αρκετά μεγάλους φυσικούς N,

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

Απόδειξη. Ο μόνος ισχυρισμός του θεωρήματος που δεν έχουμε αποδείξει ως τώρα είναι το κάτω φράγμα για την $\mathfrak{G}(N)$. 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

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

και έχουμε ολοκληρώσει την απόδειξη του θεωρήματος. □

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

Θεώρημα 4.7.11 (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-οστών δυνάμεων φυσικών αριθμών. Υπάρχει σταθερά $\delta = \delta(k,s) > 0$ τέτοια ώστε*

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

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

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

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 4.4.1, 4.5.3, 4.6.1, 4.6.3 και 4.7.10 έχουμε

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

όπου $\delta = \delta_0/k$. □

ΚΕΦΑΛΑΙΟ 5

Η μέθοδος του Linnik

5.1 Πυκνότητα κατά Schnirelmann και προσθετικές βάσεις

Στην παρούσα ενότητα πραγματευόμαστε άπειρες ακολουθίες ακεραίων, οι οποίες αρχίζουν από το μηδέν:

$$0, a_1, a_2, a_3, \dots$$

με $0 < a_1 < a_2 < \dots$ Κάποιες φορές θα θεωρούμε διαφορετικές ακολουθίες της ίδιας μορφής. Σε αυτήν την περίπτωση θα γράφουμε τους αριθμούς με δύο δείκτες, δηλαδή

$$0, a_{i,1}, a_{i,2}, a_{i,3}, \dots$$

όπου $i = 1, 2, \dots, N$. Με αυτόν τον τρόπο έχουμε δημιουργήσει N το πλήθος ακολουθίες A_i.

Αν έχουμε N το πλήθος ακολουθίες A_i, θα λέμε *άθροισμα των* A_i την ακολουθία $A_1 + A_2 + \dots + A_N$ με όρους

$$0, b_1, b_2, b_3, \dots,$$

όπου

$$b_j = a_{1,j_1} + a_{2,j_2} + \dots + a_{N,j_N}$$

είναι το άθροισμα οποιωνδήποτε N αριθμών από τις ακολουθίες, έτσι ώστε $a_{i,j_i} \in A_i$.

Συμβολίζουμε με $A^{(k)}$ την ακολουθία που προκύπτει αθροίζοντας το σύνολο A k φορές. Αν υπάρχει φυσικός αριθμός k τέτοιος ώστε $A^{(k)} = \mathbb{N}$, τότε λέμε ότι η ακολουθία A είναι *προσθετική βάση του* $\mathbb{N}$ *τάξης* k. Για παράδειγμα το θεώρημα του Lagrange φανερώνει ότι η ακολουθία των τέλειων τετραγώνων αποτελεί προσθετική βάση των φυσικών τάξης 4.

Έστω στη συνέχεια

$$A(n) = \sum_{\substack{a_i \in A \\ a_i \leqslant n}} 1$$

η αριθμητική συνάρτηση που μετρά το πλήθος των όρων μιας ακολουθίας A που δεν ξεπερνούν έναν δεδομένο φυσικό n, δίχως να προσμετρήσουμε τον αριθμό $a_0 = 0$. Τότε, όπως είναι φανερό, ισχύει

$$0 \leqslant \frac{A(n)}{n} \leqslant 1$$

για κάθε $n \in \mathbb{N}$. Η *πυκνότητα κατά Schnirelmann* της ακολουθίας A ορίζεται να είναι ο πραγματικός αριθμός

$$\sigma(A) = \inf_n \frac{A(n)}{n}.$$

Θεώρημα 5.1.1 (Schnirelmann)**.** *Έστω A, B ακολουθίες φυσικών αριθμών. Τότε*

$$\sigma(A+B) \geqslant \sigma(A) + \sigma(B) - \sigma(A)\sigma(B). \tag{5.1.1}$$

Απόδειξη. Για ευκολία γράφουμε, $\sigma(A) = \alpha$, $\sigma(B) = \beta$, $A + B = C$, $\sigma(C) = \gamma$. Επίσης θέτουμε $A(n) = \big|A \cap [1,n]\big|$, $B(n) = \big|B \cap [1,n]\big|$ και $C(n) = \big|C \cap [1,n]\big|$. Έστω a_k και a_{k+1} δύο διαδοχικοί αριθμοί στο σύνολο A. Οι αριθμοί αυτοί ανήκουν επίσης στο C. Μεταξύ των δύο αυτών αριθμών υπάρχουν ακριβώς $a_{k+1} - a_k + 1 = l$ αριθμοί οι οποίοι δεν ανήκουν στο σύνολο A, οι

$$a_k + 1, a_k + 2, \ldots, a_k + l = a_{k+1} - 1.$$

Ωστόσο κάθε αριθμός της μορφής $a_k + r$ όπου $r \in B$ και $1 \leqslant r \leqslant l$ είναι στοιχείο του συνόλου C. Είναι εύκολο να δούμε ότι το πλήθος αυτών των αριθμών είναι $B(l)$. Έτσι δείξαμε ότι κάθε διάστημα μήκους l το οποίο βρίσκεται ανάμεσα σε δύο διαδοχικά στοιχεία του συνόλου A περιέχει τουλάχιστον $B(l)$ στοιχεία του συνόλου C. Προκύπτει με αυτόν τον τρόπο ότι

$$C(n) \geqslant A(n) + \sum B(l),$$

όπου το άθροισμα εκτείνεται πάνω από όλα τα διαστήματα της μορφής (a_k, a_{k+1}), μεταξύ δύο διαδοχικών στοιχείων του συνόλου A και επίσης πάνω από τα διαστήματα $[1, a_1)$ αν $a_1 \neq 1$ και $(a_{A(n)}, n]$ αν $a_{A(n)} \neq n$. Από τον ορισμό της πυκνότητας κατά Schnirelmann έχουμε,

$$B(l) \geqslant \beta l.$$

Συμπεραίνουμε λοιπόν ότι

$$C(n) \geqslant A(n) + \sum B(l) \geqslant A(n) + \beta \sum l = A(n) + \beta(n - A(n)),$$

καθώς $\sum l = \Big|[1,a_1) \cup (a_1,a_2) \cup \cdots \cup (a_{A(n)-1}, a_{A(n)}) \cup (a_{A(n)}, n]\Big| = n - A(n)$. Όμως,

$$A(n) \geqslant \alpha n$$

και έτσι

$$C(n) \geqslant A(n) + \beta(n - A(n)) \geqslant \alpha n(1-\beta) + \beta n,$$

από το οποίο τελικά έπεται ότι

$$\frac{C(n)}{n} \geqslant \alpha + \beta - \alpha\beta$$

και το συμπέρασμα συνάγεται άμεσα. □

Παρατήρηση 5.1.2. Παρατηρούμε ότι το συμπέρασμα του παραπάνω θεωρήματος μπορεί να γραφεί ισοδύναμα στη μορφή

$$1 - \sigma(A+B) \leqslant \big(1 - \sigma(A)\big)\big(1 - \sigma(B)\big),$$

από το οποίο εύκολα, με επαγωγή στο πλήθος των όρων του αθροίσματος, συνάγουμε την σχέση

$$1 - \sigma(A_1 + A_2 + \cdots + A_k) \leqslant \prod_{i=1}^{k}(1 - \sigma(A_i))$$

ή ισοδύναμα

$$\sigma(A_1 + A_2 + \cdots + A_k) \geqslant 1 - \prod_{i=1}^{k}(1 - \sigma(A_i)).$$

Η τελευταία ανισότητα μας επιτρέπει να υπολογίζουμε την πυκνότητα κατά Schnirelmann ενός αθροίσματος, από τις πυκνότητες των προσθετέων.

Λήμμα 5.1.3. *Αν $A(n) + B(n) > n - 1$, τότε $n \in A + B$.*

Απόδειξη. Πράγματι, αν $n \in A$ ή $n \in B$ το συμπέρασμα είναι άμεσο. Συνεπώς μπορούμε να υποθέσουμε ότι το n δεν ανήκει σε κανένα από τα δύο αυτά σύνολα. Τότε, $A(n) = A(n-1)$ και $B(n) = B(n-1)$. Έπεται ότι

$$A(n-1) + B(n-1) > n - 1.$$

Έστω τώρα $a_1, a_2, \ldots, a_r$ και $b_1, b_2, \ldots, b_s$ οι αριθμοί του διάστηματος $[1, n-1]$ που ανήκουν στα σύνολα A και B αντίστοιχα. Ειδικότερα, $r = A(n-1)$ και $s = B(n-1)$. Θεωρούμε τους αριθμούς

$$a_1, a_2, \ldots, a_r, n - b_1, n - b_2, \ldots, n - b_s$$

των οποίων το πλήθος είναι $r + s = A(n-1) + B(n-1) > n - 1$ και περιέχονται όλοι στο διάστημα $[1, n-1]$. Από την αρχή της περιστεροφωλιάς υπάρχουν i,j τέτοιοι ώστε

$$a_i = n - b_j,$$

δηλαδή

$$a_i + b_j = n$$

και η απόδειξη του λήμματος ολοκληρώθηκε. □

Η Παρατήρηση 5.1.2 σε συνδυασμό με το παραπάνω λήμμα οδηγούν στο επόμενο σημαντικό θεώρημα.

Θεώρημα 5.1.4 (Schnirelmann)**.** *Κάθε ακολουθία με θετική πυκνότητα κατά Schnirelmann είναι προσθετική βάση των φυσικών αριθμών.*

Απόδειξη. Έστω $\sigma(A) = a > 0$. Για κάθε φυσικό αριθμό k θεωρούμε το σύνολο $A^{(k)}$ το οποίο είναι το άθροισμα k αντιτύπων της ακολουθίας A. Από την παρατήρηση προκύπτει ότι

$$\sigma(A^{(k)}) \geqslant 1 - (1 - a)^k.$$

Καθώς $a > 0$, υπάρχει k_0 τέτοιος ώστε

$$\sigma(A^{(k_0)}) > \frac{1}{2}.$$

Θα δείξουμε ότι η ακολουθία $A^{(2k_0)}$ περιέχει όλους τους φυσικούς αριθμούς. Προς τούτο, θεωρούμε τυχόν $n \in \mathbb{N}$. Έχουμε

$$A^{(k_0)}(n) > \frac{n}{2} > \frac{n-1}{2},$$

άρα

$$A^{(2k_0)}(n) = A^{(k_0)}(n) + A^{(k_0)}(n) > n - 1$$

και το συμπέρασμα του θεωρήματος έπεται από το προηγούμενο λήμμα. □

5.2 Λήμματα που αφορούν γραμμικές εξισώσεις

Λήμμα 5.2.1. *Έστω a_1, a_2 ακέραιοι αριθμοί για τους οποίους ισχύει $|a_2| \leqslant |a_1| \leqslant A$ και $(a_1, a_2) = 1$. Τότε, για κάθε $m \in \mathbb{Z}$, το πλήθος των λύσεων της*

$$a_1 z_1 + a_2 z_2 = m \tag{5.2.1}$$

με τον περιορισμό $|z_i| \leqslant A$ για $i = 1, 2$ δεν ξεπερνά τον αριθμό $3A/|a_1|$.

Απόδειξη. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $a_1 > 0$, αλλιώς αντικαθιστούμε τον z_1 στην εξίσωση με $-z_1$. Έστω $(z_1, z_2), (z_1', z_2')$ δύο διαφορετικές λύσεις της εξίσωσης (5.2.1). Έχουμε λοιπόν ότι

$$a_1 z_1 + a_2 z_2 = m$$

και

$$a_1 z_1' + a_2 z_2' = m,$$

συνεπώς προκύπτει η σχέση

$$a_1(z_1 - z_1') = a_2(z_2 - z_2').$$

Επίσης, $(a_1, a_2) = 1$ και άρα παίρνουμε $z_2 - z_2' \equiv 0 \bmod a_1$, και συνεπώς $|z_2 - z_2'| \geqslant a_1$. Εύκολα βλέπουμε ότι το πλήθος των λύσεων (z_1, z_2) της (5.2.1) υπό τον περιορισμό $|z_i| \leqslant A$ για $i = 1, 2$ δεν ξεπερνά το πλήθος t των z_2 για τους οποίους $|z_2| \leqslant A$ και υπάρχει z_1 με $|z_1| \leqslant A$ ώστε το (z_1, z_2) να είναι λύση της (5.2.1). Αφού δείξαμε ότι η απόσταση δύο τέτοιων αριθμών είναι πολλαπλάσιο του αριθμού a_1 έπεται ότι

$$a_1(t-1) \leqslant 2A,$$

δηλαδή

$$t \leqslant \frac{2A}{a_1} + 1 \leqslant \frac{3A}{a_1}$$

και η απόδειξη ολοκληρώθηκε. □

Λήμμα 5.2.2. *Έστω $a_1, a_2, \ldots, a_\ell$ ακέραιοι αριθμοί για τους οποίους ισχύει $|a_i| \leqslant A$ για κάθε $i = 1, 2, \ldots, \ell$ και $(a_1, a_2, \ldots, a_\ell) = 1$. Τότε, για κάθε $m \in \mathbb{Z}$, το πλήθος των λύσεων της εξίσωσης*

$$a_1 z_1 + \cdots + a_\ell z_\ell = m \tag{5.2.2}$$

με $|z_i| \leqslant A$ για $i = 1, 2, \ldots, \ell$ δεν ξεπερνά τον αριθμό $cA^{\ell-1}/H$ όπου $H = \max |a_i|$ και c μία σταθερά η οποία εξαρτάται μόνο από το ℓ.

Απόδειξη. Αποδεικνύεται με επαγωγή στο ℓ. Η περίπτωση $\ell = 2$ είναι το Λήμμα 5.2.1 με $c = 3$. Υποθέτουμε ότι το συμπέρασμα αληθεύει στην περίπτωση των $\ell - 1$ αγνώστων. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $|a_\ell| = \max |a_i|$. Διακρίνουμε περιπτώσεις:

(1) Αν $a_1 = a_2 = \cdots = a_{\ell-1} = 0$ τότε καθώς $(a_1, a_2, \ldots, a_\ell) = 1$, έχουμε αναγκαστικά $a_\ell = \pm 1$ και η (5.2.2) είναι της μορφής $\pm z_\ell = m$. Είναι φανερό λοιπόν ότι κάθε ένας από τους αγνώστους $z_1, z_2, \ldots, z_{\ell-1}$ μπορεί να πάρει οποιαδήποτε ακέραια τιμή στο διάστημα $[-A, A]$, δηλαδή συνολικά $2A + 1 \leqslant 3A$ τιμές. Από την άλλη πλευρά, ο z_ℓ μπορεί να πάρει ακριβώς μία τιμή. Συνεπώς, το συνολικό πλήθος των λύσεων της εξίσωσης (5.2.2) δεν ξεπερνά τον αριθμό

$$(3A)^{\ell-1} = \frac{cA^{\ell-1}}{H},$$

όπου $c = 3^{\ell-1}$ και $H = |a_\ell| = 1$.

(2) Αν τώρα κάποιος από τους $a_1, a_2, \ldots, a_{\ell-1}$ είναι μη μηδενικός, θεωρούμε τον μέγιστο κοινό τους διαιρέτη δ. Έστω επίσης

$$H' = \frac{\max |a_i|}{\delta}$$

για $i \leqslant \ell - 1$. Υποθέτουμε ότι αριθμοί $z_1, z_2, \ldots, z_\ell$ ικανοποιούν την αρχική εξίσωση καθώς και τις ανισότητες $|z_i| \leqslant A$ για $i = 1, 2, \ldots, \ell$. Θέτουμε

$$\left(\frac{a_1}{\delta}\right) z_1 + \left(\frac{a_2}{\delta} z_2\right) + \cdots + \left(\frac{a_{\ell-1}}{\delta} z_{\ell-1}\right) = m', \tag{5.2.3}$$

και άρα

$$a_1 z_1 + a_2 z_2 + \cdots + a_{\ell-1} z_{\ell-1} = \delta m',$$

ώστε

$$\delta m' + a_\ell z_\ell = m. \tag{5.2.4}$$

Ισχύει

$$|\delta m'| \leqslant \sum_{i=1}^{\ell-1} |a_i||z_i| \leqslant \ell \delta H' A$$

και έτσι

$$|m'| \leqslant \ell H' A.$$

Αντικαταστήσαμε λοιπόν την εξίσωση (5.2.2) με τις εξισώσεις (5.2.3) και (5.2.4). Τώρα στην εξίσωση (5.2.4) έχουμε $\delta \leqslant |a_\ell|$ και $(\delta, a_\ell) = (a_1, a_2, \ldots, a_\ell) = 1$. Από το Λήμμα 5.2.1 συμπεραίνουμε ότι ο αριθμός των λύσεων της εξίσωσης (5.2.4) με $|m'| \leqslant \ell H' A$ και $|z_\ell| \leqslant A \leqslant \ell H' A$ δεν ξεπερνά τον $3\ell H' A/|a_\ell|$. Για αυτό το m', η εξίσωση (5.2.3) από την επαγωγική υπόθεση έχει λιγότερες από $c' A^{\ell-2}/H'$ λύσεις στους ακέραιους z_i για $i = 1, 2, \ldots, \ell - 1$ με $|z_i| \leqslant A$. Έπεται λοιπόν ότι ο αριθμός των λύσεων της αρχικής εξίσωσης δεν ξεπερνά τον

$$\frac{3\ell H' A}{|a_\ell|} \frac{c' A^{\ell-2}}{H'} = \frac{3\ell c' A^{\ell-1}}{|a_\ell|} = \frac{cA^{\ell-1}}{H},$$

όπου $c = 3\ell c'$, $H = |a_\ell|$ και η απόδειξη ολοκληρώθηκε. □

Λήμμα 5.2.3. *Έστω $\ell > 2$ και $1 \leqslant A \leqslant B \leqslant c(\ell)A^{\ell-1}$. Τότε το άθροισμα του πλήθους των λύσεων, με $|z_i| \leqslant B$ για $i = 1, 2, \ldots, \ell$, όλων των εξισώσεων της μορφής*

$$a_1 z_1 + a_2 z_2 + \cdots + a_\ell z_\ell = 0, \tag{5.2.5}$$

όπου $|a_i| \leqslant A$ για $i = 1, 2, \ldots, \ell$, δεν ξεπερνά τον αριθμό

$$c(\ell)(AB)^{\ell-1},$$

όπου $c(\ell)$ σταθερά η οποία εξαρτάται μόνο από το ℓ.

Απόδειξη. Θα διακρίνουμε πάλι περιπτώσεις:

(1) Έστω ότι $a_1 = a_2 = \cdots = a_\ell = 0$. Σε αυτήν την περίπτωση, αφού $z_i \in [-B, B]$ για $1 \leqslant i \leqslant \ell$, εύκολα βλέπουμε ότι το πλήθος των λύσεων $(z_1, z_2, \ldots, z_\ell)$ της (5.2.5) δεν ξεπερνά τον αριθμό

$$(2B+1)^\ell \leqslant (3B)^\ell = 3^\ell B^\ell = 3^\ell c(\ell) B^{\ell-1} A^{\ell-1} = c(\ell)(AB)^{\ell-1}.$$

(2) Αν τουλάχιστον ένας εκ των συντελεστών a_i είναι μη μηδενικός, και

$$(a_1, a_2, \ldots, a_\ell) = \delta = 1,$$

τότε θέτουμε

$$H = \max |a_i|.$$

Ισχύει $H \in [1, A]$, άρα μπορούμε να βρούμε έναν ακέραιο m τέτοιον ώστε

$$\frac{A}{2^{m+1}} < H \leqslant \frac{A}{2^m}. \tag{5.2.6}$$

Για μία οποιαδήποτε εξίσωση της μορφής (5.2.5), όπου $\delta = 1$ και το H ικανοποιεί την ανισότητα (5.2.6), το πλήθος των λύσεων $(z_1, z_2, \ldots, z_\ell)$ με $|z_i| \leqslant B$ για $1 \leqslant i \leqslant \ell$, δεν ξεπερνά, από το Λήμμα 5.2.2, τον αριθμό

$$c(\ell)\frac{B^{\ell-1}}{H} \leqslant c(\ell)\frac{B^{\ell-1}}{\frac{A}{2^{m+1}}} = c(\ell)\frac{B^{\ell-1}2^m}{A}.$$

Επιπλέον, από την (5.2.6) συμπεραίνουμε ότι $|a_i| \leqslant A/2^m$ για κάθε $i \in \{1, \ldots, \ell\}$. Συνεπώς, ο συνολικός αριθμός των εξισώσεων που ικανοποιούν την σχέση (5.2.6), δεν ξεπερνά τον αριθμό

$$\left(2\frac{A}{2^m} + 1\right)^\ell \leqslant \left(3\frac{A}{2^m}\right)^\ell = c(\ell)A^\ell 2^{-m\ell}.$$

Προκύπτει ότι ο αντίστοιχος αριθμός λύσεων όλων των εξισώσεων που ικανοποιούν τίς παραπάνω συνθήκες δεν ξεπερνά τον αριθμό

$$c(\ell)\frac{B^{\ell-1}2^m}{A}c(\ell)A^\ell 2^{-m\ell} = c(\ell)(AB)^{\ell-1}2^{-(\ell-1)m}.$$

Αθροίζοντας τώρα για όλα τα $m \geqslant 0$ βρίσκουμε το συνολικό άνω φράγμα

$$\sum_{m=0}^{k} c(\ell)(AB)^{\ell-1}2^{-(\ell-1)m} = c(\ell)(AB)^{\ell-1}\sum_{m=0}^{k} 2^{-(\ell-1)m} = c(\ell)(AB)^{\ell-1},$$

καθώς $\ell > 2$.

(3) Τέλος, υποθέτουμε ότι τουλάχιστον ένας εκ των συντελεστών a_i, είναι μη μηδενικός, και

$$(a_1, a_2, \ldots, a_\ell) = \delta > 1.$$

Σε αυτήν την περίπτωση αντικαθιστούμε την εξίσωση (5.2.5) με την

$$\frac{a_1}{\delta} z_1 + \cdots + \frac{a_\ell}{\delta} z_\ell = 0,$$

όπου $\left(\frac{a_1}{\delta}, \ldots, \frac{a_\ell}{\delta}\right) = 1$. Ο αριθμός A αντικαθίσταται έτσι από τον μικρότερο αριθμό A/δ. Η συνθήκη $B = c(\ell)A^{\ell-1}$ με αυτόν τον τρόπο παραβιάζεται, ωστόσο μας χρειάστηκε μόνο στην απόδειξη της πρώτης περίπτωσης. Από την δεύτερη περίπτωση, για το συγκεκριμένο δ και για $|z_i| \leqslant A$, βλέπουμε ότι το συνολικό πλήθος των λύσεων των εξισώσεων της μορφής (5.2.5), δεν ξεπερνά τον αριθμό

$$c(\ell)\Big(\frac{A}{\delta}B\Big)^{\ell-1} = c(\ell)\frac{(AB)^{\ell-1}}{\delta^{\ell-1}}. \tag{5.2.7}$$

Επιπλέον, $\delta \leqslant A$. Έτσι αθροίζοντας πάνω από όλα τα δυνατά δ παίρνουμε το συνολικό άνω φράγμα

$$c(\ell)(AB)^{\ell-1}\sum_{\delta=1}^{A}\frac{1}{\delta^{\ell-1}}. \tag{5.2.8}$$

Αφού $\ell > 2$, έχουμε

$$\sum_{\delta=1}^{A}\frac{1}{\delta^{\ell-1}} < \sum_{\delta=1}^{\infty}\frac{1}{\delta^2} = \frac{\pi^2}{6}.$$

Συνεπώς έχουμε το άνω φράγμα

$$c(\ell)(AB)^{\ell-1}. \tag{5.2.9}$$

Συνδυάζοντας αυτό το φράγμα με το αποτέλεσμα της πρώτης περίπτωσης έχουμε το ζητούμενο άνω φράγμα. □

Στην συνέχεια θεωρούμε πεπερασμένα σύνολα ακεραίων αριθμών στα οποία η επανάληψη στοιχείων είναι επιτρεπτή. Αν ο ακέραιος αριθμός a εμφανίζεται στο σύνολο A, λ φορές, λέμε ότι η πολλαπλότητά του στο A είναι $\lambda = \lambda(a)$.

Λήμμα 5.2.4. *Έστω c ακέραιος αριθμός και A, B πεπερασμένα σύνολα ακεραίων αριθμών. Αν N_1 είναι το πλήθος των λύσεων της εξίσωσης*

$$x + y = c \tag{5.2.10}$$

με $x \in A$ και $y \in B$, N_2 το πλήθος των λύσεων της εξίσωσης

$$x - y = 0$$

με $x \in A$ και $y \in A$, και N_3 το πλήθος των λύσεων της εξίσωσης

$$x - y = 0$$

με $x \in B$ και $y \in B$, τότε ισχύει

$$N_1 \leqslant N_2 + N_3.$$

Απόδειξη. Έστω $a_1, a_2, \dots, a_n$ και $= b_1, b_2, \dots, b_m$ οι ανά δύο διαφορετικοί αριθμοί που εμφανίζονται στα A, B αντίστοιχα. Παρατηρούμε ότι για κάθε x στο A υπάρχει το πολύ μία τιμή y_x στο B τέτοια ώστε

$$x - y_x = c.$$

Αν τώρα η πολλαπλότητα του $x = a_i$ είναι λ_i και η πολλαπλότητα του $y_x = b_k$ είναι μ_k, τότε έχουμε $\lambda_i \mu_k$ λύσεις της εξίσωσης (5.2.10). Όμως,

$$\lambda_i \mu_k \leqslant \frac{1}{2}(\lambda_i^2 + \mu_k^2)$$

και έτσι έπεται ότι

$$N_1 \leqslant \sum \frac{1}{2}(\lambda_i^2 + \mu_k^2),$$

όπου το άθροισμα εκτείνεται πάνω από όλα τα ζεύγη δεικτών $\{i, k\}$ για τα οποία $a_i + b_k = c$. Είναι προφανές τώρα ότι

$$N_1 \leqslant \sum \frac{1}{2}(\lambda_i^2 + \mu_k^2) \leqslant \frac{1}{2}\Big(\sum_{i=1}^{n} \lambda_i^2 + \sum_{k=1}^{m} \mu_k^2\Big).$$

Από την άλλη πλευρά βλέπουμε ότι κάθε λύση της εξίσωσης

$$x - y = 0,$$

όπου $x \in A$ και $y \in A$, είναι της μορφής $x = y = a_i$ για κάποιο $1 \leqslant i \leqslant n$. Συνεπώς, για κάθε i έχουμε λ_i λύσεις της εξίσωσης αυτής και άρα συμπεραίνουμε ότι

$$N_2 = \sum_{i=1}^{n} \lambda_i^2.$$

Αντίστοιχα προκύπτει ότι

$$N_3 = \sum_{k=1}^{m} \mu_k^2$$

και το ζητούμενο έπεται άμεσα. □

Το επόμενο πόρισμα αποτελεί ειδική περίπτωση του λήμματος για $A = B$.

Πόρισμα 5.2.5. *Το πλήθος των λύσεων της εξίσωσης*

$$x + y = c,$$

όπου $x \in A$ και $y \in A$, δεν ξεπερνά το πλήθος των λύσεων της εξίσωσης

$$x - y = 0,$$

όπου $x \in A$ και $y \in A$.

Έστω τώρα k και τ δύο αυθαίρετοι φυσικοί αριθμοί. Θέτουμε $\ell = k2^\tau$, και μελετάμε την εξίσωση

$$x_1 + x_2 + \cdots + x_\ell = c.$$

Έστω $A_1, A_2, \ldots, A_\ell$ πεπερασμένα σύνολα ακεραίων. Υποθέτουμε ότι κάθε σύνολο A_i για $1 \leqslant i \leqslant \ell$ αποτελείται από τους διαφορετικούς ανά δύο αριθμούς $a_{i1}, a_{i2}, \ldots$ με αντίστοιχες πολλαπλότητες $\lambda_{i1}, \lambda_{i2}, \ldots$. Ενδιαφερόμαστε για το πλήθος των λύσεων της εξίσωσης

$$x_1 + x_2 + \cdots + x_\ell = c,$$

όπου $x_i \in A_i$ για $1 \leqslant i \leqslant \ell$.

Γενικεύοντας το Λήμμα 5.2.4 έχουμε το ακόλουθο:

Λήμμα 5.2.6. *Έστω $\ell = k2^\tau$. Αν N είναι το πλήθος των λύσεων της εξίσωσης*

$$x_1 + x_2 + \cdots + x_\ell = c \tag{5.2.11}$$

όπου $x_i \in A_i$, για $1 \leqslant i \leqslant \ell$, και N_m το πλήθος των λύσεων της εξίσωσης

$$y^{(1)} + y^{(2)} + \cdots + y^{(2^{\tau-1})} - y^{(2^{\tau-1}+1)} - \cdots - y^{(2^\tau)} = 0,$$

όπου

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \cdots + y_k^{(j)}$$

και

$$y_1^{(j)} \in A_{mk+1}, y_2^{(j)} \in A_{mk+2}, \ldots, y_k^{(j)} \in A_{(m+1)k}$$

για $j = 1, 2, \ldots, 2^\tau$, τότε

$$N \leqslant N_1 + N_2 + \cdots + N_{2^\tau}.$$

Απόδειξη. Αν θέσουμε $x_1 + x_2 + \cdots + x_{\ell/2} = x$ και $x_{\ell/2+1} + \cdots + x_\ell = y$ τότε η δοσμένη εξίσωση μπορεί να γραφτεί ως

$$x + y = c,$$

και έτσι μπορούμε να εφαρμόσουμε το Λήμμα 5.2.4. Ο x μπορεί να είναι οποιοσδήποτε αριθμός της μορφής $z_1 + z_2 + \cdots + z_{\ell/2}$, όπου $z_i \in A_i$ για $1 \leqslant i \leqslant \ell/2$. Όμοια, ο y μπορεί να είναι οποιοσδήποτε αριθμός της μορφής $z_1 + z_2 + \cdots + z_{\ell/2}$, όπου τώρα $z_i \in A_{i+\ell/2}$ για $1 \leqslant i \leqslant \ell/2$.

Από το Λήμμα 5.2.4, με $A = A_1 + A_2 + \cdots + A_{\ell/2}$ και $B = A_{\ell/2+1} + A_{\ell/2+2} + \cdots + A_\ell$, βλέπουμε ότι ο N δεν ξεπερνά το πλήθος των λύσεων της

$$x - y = 0 \tag{5.2.12}$$

με τις ακόλουθες δύο υποθέσεις:

$$\begin{aligned} x &= z_1 + z_2 + \cdots + z_{\ell/2}, \\ y &= z'_1 + z'_2 + \cdots + z'_{\ell/2}, \end{aligned} \tag{5.2.13}$$

όπου $z_i \in A_i, z_i' \in A_i$ για $1 \leqslant i \leqslant \ell/2$, και

$$x = z_1 + z_2 + \cdots + z_{\ell/2}, \tag{5.2.14}$$
$$y = z_1' + z_2' + \cdots + z_{\ell/2}',$$

όπου $z_i \in A_{i+\ell/2}$ και $z_i' \in A_{i+\ell/2}$ για $1 \leqslant i \leqslant \ell/2$. Και στις δύο περιπτώσεις, η εξίσωση (5.2.11) μπορεί να γραφτεί στη μορφή

$$(z_1 - z_1') + (z_2 - z_2') + \cdots + (z_{\ell/2} - z_{\ell/2}') = 0. \tag{5.2.15}$$

Έτσι συμπεραίνουμε ότι ο N δεν ξεπερνά το μισό του αθροίσματος του πλήθους των λύσεων της (5.2.15) υπό τις δύο προϋποθέσεις, δηλαδή δεν ξεπερνά το μισό του αθροίσματος του πλήθους των λύσεων των εξισώσεων

$$\sum_{i=1}^{\ell/2}(z_i - z_i') = 0,$$

όπου $z_i \in A_i$ και $z_i' \in A_i$ για $1 \leqslant i \leqslant \ell/2$, και

$$\sum_{i=1}^{\ell/2}(z_i - z_i') = 0,$$

όπου $z_i \in A_{i+\ell/2}$ και $z_i' \in A_{i+\ell/2}$ για $1 \leqslant i \leqslant \ell/2$.

Η εξίσωση (5.2.15) έχει $\frac{1}{2}\ell$ όρους στο αριστερό μέλος, δηλαδή τους μισούς της αρχικής εξίσωσης (5.2.11). Θέτοντας

$$\sum_{i=1}^{\ell/4}(z_i - z_i') = x$$

και

$$\sum_{i=\ell/4+1}^{\ell/2}(z_i - z_i') = y,$$

η (5.2.15) γράφεται στη μορφή

$$x + y = 0,$$

και μπορούμε να εφαρμόσουμε πάλι το Λήμμα 5.2.4. Εργαζόμενοι με τον ίδιο ακριβώς τρόπο, που μας οδήγησε από την (5.2.11) στην (5.2.15), τώρα από την (5.2.15) φτάνουμε στην

$$\sum_{i=1}^{\ell/4}(u_i + u_i' - u_i'' - u_i''') = 0, \tag{5.2.16}$$

όπου τώρα θεωρούμε το άθροισμα του πλήθους των λύσεων της υπό τις εξής υποθέσεις:

$$u_i, u_i', u_i'', u_i''' \in A_i \tag{5.2.17}$$
$$u_i, u_i', u_i'', u_i''' \in A_{\ell/4+i} \tag{5.2.18}$$
$$u_i, u_i', u_i'', u_i''' \in A_{\ell/2+i} \tag{5.2.19}$$
$$u_i, u_i', u_i'', u_i''' \in A_{3\ell/4+i} \tag{5.2.20}$$

για

$$1 \leqslant i \leqslant \frac{\ell}{4}.$$

Καθώς $\ell = k2^\tau$, μπορούμε να επαναλάβουμε την παραπάνω διαδικασία τ φορές. Ως αποτέλεσμα, παίρνουμε την εξίσωση

$$\sum_{i=1}^{k} \left(y_i^{(1)} + y_i^{(2)} + \cdots + y_i^{(2^{\tau-1})} - y_i^{(2^{\tau-1}+1)} - \cdots - y_i^{(2^\tau)}\right) = 0, \tag{5.2.21}$$

όπου τώρα θεωρούμε το συνολικό πλήθος των λύσεων της (5.2.21) υπό τις εξής 2^τ υποθέσεις:

$$\begin{aligned} &y_1^{(j)} \in A_1, y_2^{(j)} \in A_2, \ldots, y_k^{(j)} \in A_k, \\ &y_1^{(j)} \in A_{k+1}, y_2^{(j)} \in A_{k+2}, \ldots, y_k^{(j)} \in A_{2k}, \\ &\qquad \vdots \\ &y_1^{(j)} \in A_{k2^\tau-k+1}, \ldots, y_k^{(j)} \in A_{k2^\tau} \end{aligned}$$

για

$$1 \leqslant j \leqslant 2^\tau.$$

Θέτοντας

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \cdots + y_k^{(j)}$$

για $1 \leqslant j \leqslant 2^\tau$, η εξίσωση (5.2.21) παίρνει την απλή μορφή

$$y^{(1)} + y^{(2)} + \cdots + y^{(2^{\tau-1})} - y^{(2^{\tau-1}+1)} - \cdots - y^{(2^\tau)} = 0. \tag{5.2.22}$$

Εδώ μιλάμε για το συνολικό πλήθος των λύσεων της εξίσωσης (5.2.22) υπό τις ακόλουθες υποθέσεις, οι οποίες διαφέρουν η μία από την άλλη στις τιμές της παραμέτρου m, για $0 \leqslant m \leqslant 2^\tau - 1$:

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \cdots + y_k^{(j)},$$

όπου

$$y_1^{(j)} \in A_{mk+1}, y_2^{(j)} \in A_{mk+2}, \ldots, y_k^{(j)} \in A_{(m+1)k}$$

για $1 \leqslant j \leqslant 2^\tau$. Έπεται λοιπόν ότι

$$N \leqslant N_1 + N_2 + \cdots + N_{2^\tau},$$

και η απόδειξη είναι πλήρης. □

5.3 Το κύριο λήμμα

Έστω A_k η ακολουθία των k-οστών δυνάμεων, και έστω $A_k^{(s)}$ το άθροισμα s αντιτύπων της A_k. Αν μπορούσαμε να δείξουμε ότι για επαρκώς μεγάλο s, το σύνολο $A_k^{(s)}$ έχει θετική πυκνότητα κατά Schnirelmann, τότε το Θεώρημα 5.1.4 μας εξασφαλίζει ότι το σύνολο των k-οστών δυνάμεων αποτελεί προσθετική βάση του $\mathbb{N}$, δηλαδή το πρόβλημα του Waring έχει καταφατική απάντηση για κάθε k.

Έστω N θετικός ακέραιος. Θεωρούμε την εξίσωση

$$x_1^k + \cdots + x_s^k = N, \tag{5.3.1}$$

όπου $x_i \geqslant 0$. Έστω $r_{k,s}(N)$ το πλήθος των λύσεων της εξίσωσης (5.3.1). Στα παρακάτω θεώρούμε τον $k \geqslant 2$ σταθερό. Διατυπώνουμε το *κύριο λήμμα*:

Λήμμα 5.3.1 (κύριο λήμμα)**.** *Υπάρχει $s = s(k)$ τέτοιος ώστε, για κάθε $N \geqslant 1$, να ισχύει*

$$r_{k,s}(m) \leqslant cN^{\frac{s}{k}-1}, \tag{5.3.2}$$

για $1 \leqslant m \leqslant N$, όπου η σταθερά c εξαρτάται μόνο από το k.

Δείχνουμε ότι από το Λήμμα 5.3.1 έπεται ότι $\sigma(A_k^{(s)}) > 0$. Γνωρίζουμε ότι

$$r_{k,s}(0) + r_{k,s}(1) + \cdots + r_{k,s}(N) = R_{k,s}(N),$$

όπου $R_{k,s}(N)$ είναι το πλήθος των λύσεων της ανίσωσης

$$x_1^k + \cdots + x_s^k \leqslant N. \tag{5.3.3}$$

Παρατηρούμε ότι όταν

$$0 \leqslant x_i \leqslant \left(\frac{N}{s}\right)^{\frac{1}{k}},$$

για κάθε $1 \leqslant i \leqslant s$, τότε οι αριθμοί $(x_1, x_2, \ldots, x_s)$ αποτελούν λύση της (5.3.3). Συνεπώς έχουμε

$$R_{k,s}(N) \geqslant \left(\frac{N}{s}\right)^{\frac{s}{k}}. \tag{5.3.4}$$

Υποθέτουμε ότι $\sigma(A_k^{(s)}) = 0$. Σε αυτήν την περίπτωση, για κάθε $\varepsilon > 0$, μπορούμε να βρούμε $N = N(\varepsilon)$ ώστε

$$A_k^{(s)}(N) < \varepsilon N.$$

Από την (5.3.2) παίρνουμε

$$R_{k,s}(N) = \sum_{m=0}^{N} r_{k,s}(m) = r_{k,s}(0) + \sum_{m=1}^{N} r_{k,s}(m) < 1 + cN^{\frac{s}{k}-1} A_k^{(s)}(N) < 1 + c\varepsilon N^{\frac{s}{k}},$$

το οποίο για επαρκώς μικρό ε, αντιφάσκει με την (5.3.4). Έτσι, $\sigma(A_k^{(s)}) > 0$.

Επιστρέφουμε στην απόδειξη του κύριου λήμματος. Θα το αποδείξουμε με επαγωγή στο k. Για να καταφέρουμε να μεταβούμε από το $k-1$ στο k, αντί για την αρχική εξίσωση

$$x_1^k + \cdots + x_s^k = m,$$

με $m \leqslant N$, του προβλήματος του Waring, όπου $x_i \geqslant 0$, έτσι ώστε $x_i \leqslant m^{1/k} \leqslant N^{1/k}$, θα μελετήσουμε την εξίσωση

$$f(x_1) + f(x_2) + \cdots + f(x_s) = m \tag{5.3.5}$$

με $m \leqslant N$, όπου το $f(x) = a_0x^k + a_1x^{k-1} + \cdots + a_{k-1}x + a_k$ είναι ένα πολυώνυμο με $a_0 \neq 0$ και το οποίο μπορεί να εξαρτάται από το k και το N με τέτοιον τρόπο ώστε να ικανοποιείται η σχέση

$$|a_i| \leqslant cN^{\frac{i}{k}} \tag{5.3.6}$$

για $0 \leqslant i \leqslant k$. Η σταθερά c εξαρτάται μόνο από το k. Το κύριο Λήμμα 5.3.1 θα προκύψει ως συνέπεια του παρακάτω γενικότερου λήμματος:

Λήμμα 5.3.2. *Υπάρχει $s = s(k)$ τέτοιος ώστε το πλήθος των λύσεων $(x_1, x_2, \ldots, x_s)$ της (5.3.5) με την επιπλέον υπόθεση ότι $|x_i| \leqslant N^{1/k}$ για κάθε $1 \leqslant i \leqslant s$, δεν ξεπερνά τον αριθμό*

$$cN^{\frac{s}{k}-1} \tag{5.3.7}$$

για κάθε $1 \leqslant m \leqslant N$, όπου c σταθερά η οποία εξαρτάται μόνο από το k.

Απόδειξη. Αρχικά δείχνουμε το ζητούμενο για $k = 1$. Τότε θα έχουμε $f(x) = a_0x + a_1$. Θέτουμε $s(1) = 2$, και έτσι η εξίσωση (5.3.5) παίρνει τη μορφή

$$a_0(x_1 + x_2) = m - 2a_1, \tag{5.3.8}$$

και $|x_i| \leqslant N$ για $i = 1, 2$. Εφόσον $|x_1| \leqslant N$ υπάρχουν $2N + 1 \leqslant 3N$ πιθανές τιμές για το x_1, και για κάθε μία από αυτές υπάρχει το πολύ μία τιμή για το x_2, ώστε να ικανοποιείται η εξίσωση (5.3.8). Έτσι το συνολικό πλήθος λύσεων δεν ξεπερνά τον αριθμό $3N$, το οποίο και αποδεικνύει το λήμμα στην περίπτωση $k = 1$.

Στην συνέχεια έστω $k > 0$ και υποθέτουμε ότι το λήμμα ισχύει για τον $k - 1$. Θέτουμε $s(k-1) = s'$ και $s = s(k) = (2k)2^{\tau+1}$, όπου $\tau = [4 \ln_2 s'] - 1$. Εφαρμόζουμε το Λήμμα 5.2.5 στην εξίσωση (5.3.5). Θέτουμε δηλαδή

$$x = \sum_{i=1}^{s/2} f(x_i) \quad \text{και} \quad y = \sum_{s/2+1}^{s} f(x_i). \tag{5.3.9}$$

Από το Λήμμα 5.2.5 τώρα, έχουμε ότι ο $r_{k,s}^{(f)}(m)$ δεν ξεπερνά το πλήθος των λύσεων της εξίσωσης $x - y = 0$, όπου οι x, y δίνονται από την σχέση (5.3.9) και επίσης $|x_i| \leqslant N^{1/k}$, $|y_i| = |x_{i+s/2}| \leqslant N^{1/k}$ για $1 \leqslant i \leqslant s/2$. Δηλαδή ο $r_{k,s}^{(f)}(m)$ δεν ξεπερνά το πλήθος των λύσεων της εξίσωσης

$$\sum_{i=1}^{s/2} \big(f(x_i) - f(y_i)\big) = 0 \tag{5.3.10}$$

με τους περιορισμούς για τα $|x_i|, |y_i|$ που δόθηκαν παραπάνω. Κάνουμε αλλαγή μεταβλητής στην (5.3.10) θέτοντας $x_i = y_i + h_i$ και εξετάζουμε πλέον το σύστημα των αριθμών (y_i, h_i) για $1 \leqslant i \leqslant s/2$, όπου όμως επιτρέπουμε στους y_i, h_i να πάρουν αυθαίρετες τιμές στο σύνολο $[-2N^{1/k}, 2N^{1/k}]$. Αυτό μπορεί να οδηγήσει μόνο σε αύξηση του πλήθους λύσεων της (5.3.10) και άρα δεν δημιουργεί πρόβλημα στην απόδειξη. Κάθε όρος της (5.3.10) μετατρέπεται τώρα στον όρο

$$f(y_i + h_i) - f(y_i) = \sum_{\upsilon=0}^{k-1} a_\upsilon \big((y_i + h_i)^{k-\upsilon} - y_i^{k-\upsilon}\big) = \sum_{\upsilon=0}^{k-1} a_\upsilon \sum_{t=1}^{k-\upsilon} \binom{k-\upsilon}{t} h_i^t y_i^{k-\upsilon-t}.$$

Αν αλλάξουμε τη μεταβλητή της άθροισης t, θέτοντας

$$u = \upsilon + t,$$

έτσι ώστε

$$k - \upsilon - t = k - u \ \ \kappa\alpha\iota \ \ t = u - \upsilon,$$

παίρνουμε

$$\begin{aligned} f(y_i + h_i) - f(y_i) &= \sum_{\upsilon=0}^{k-1} a_\upsilon \sum_{t=1}^{k-\upsilon} \binom{k-\upsilon}{t} h_i^t y_i^{k-\upsilon-t} \\ &= h_i \sum_{\upsilon=0}^{k-1} a_\upsilon \sum_{u=\upsilon+1}^{k} \binom{k-u}{u-\upsilon} h_i^{u-\upsilon-1} y_i^{k-u} \\ &= h_i \sum_{u=1}^{k} y_i^{k-u} \sum_{\upsilon=0}^{u-1} a_\upsilon \binom{k-u}{u-\upsilon} h_i^{u-\upsilon-1} \\ &= h_i \sum_{u=1}^{k} a_{i,u} y_i^{k-u} \\ &= h_i \varphi_i(y_i), \end{aligned}$$

όπου

$$\varphi_i(y) = \sum_{u=1}^{k} a_{i,u} y^{k-u}$$

είναι ένα πολυώνυμο βαθμού $k-1$ με συντελεστές

$$a_{i,u} = \sum_{\upsilon=0}^{u-1} a_\upsilon \binom{k-u}{u-\upsilon} h_i^{u-\upsilon-1},$$

για $1 \leqslant i \leqslant s/2$, οι οποίοι εξαρτώνται από τους αριθμούς h_i.

Έτσι, με τις νέες μεταβλητές $\{y_i, h_i\}$, η εξίσωση (5.3.10) παίρνει τη μορφή

$$h_1\varphi_1(y_1) + h_2\varphi_2(y_2) + \cdots + h_{s/2}\varphi_{s/2}(y_{s/2}) = 0 \tag{5.3.11}$$

Σε αυτήν την εξίσωση, οι αριθμοί y_i και h_i μπορούν να πάρουν αυθαίρετες τιμές στο διάστημα $[-2N^{1/k}, 2N^{1/k}]$ και οι συντελεστές του πολυωνύμου $\varphi_i(y)$ εξαρτώνται από τους αριθμούς h_i. Σε αυτό το σημείο ας δούμε τι έχουμε αποδείξει ως τώρα:

Ο αριθμός $r_{k,s}^{(f)}(m)$ δεν ξεπερνά το άθροισμα του πλήθους των λύσεων στους ακεραίους y_i, $|y_i| \leqslant 2N^{1/k}$ για $1 \leqslant i \leqslant s/2$, όλων των εξισώσεων της μορφής (5.3.11)*, που μπορούν να προκύψουν από όλες τις πιθανές τιμές των αριθμών h_i με $|h_i| \leqslant 2N^{1/k}$ για $1 \leqslant i \leqslant s/2$.*

Στη συνέχεια εξετάζουμε μία εξίσωση της μορφής (5.3.11), δηλαδή θεωρούμε τους αριθμούς $h_1, h_2, \ldots, h_{s/2}$ σταθερούς και θέλουμε να βρούμε ένα άνω φράγμα για το πλήθος λύσεων στους y_i της εξίσωσης αυτής. Θα εφαρμόσουμε το Λήμμα 5.2.6, όπου στη θέση του x_i έχουμε τους αριθμούς $y_i\varphi_i(y_i)$ και στη θέση του ℓ έχουμε τον $s/2 = (2k)2^\tau$, $k_0 = 2k$.

Τα σύνολα A_i αποτελούνται από τους αριθμούς $x_i = h_i\varphi_i(y_i)$, όπου οι αριθμοί h_i θεωρούνται δεδομένοι και για τους y_i έχουμε $|y_i| \leqslant 2N^{1/k}$.

Από το Λήμμα 5.2.6, και υπό αυτές τις συνθήκες, το πλήθος των λύσεων της εξίσωσης (5.3.11) δεν ξεπερνά το πλήθος των λύσεων της

$$y^{(1)} + y^{(2)} + \cdots + y^{(2^{\tau-1})} - y^{(2^{\tau-1}+1)} - \cdots - y^{(2^\tau)} = 0 \tag{5.3.12}$$

με 2^τ πιθανές συνθήκες, οι οποίες σχετίζονται με τις τιμές της παραμέτρου $\mu = 0, 1, \ldots, 2^\tau - 1$:

$$\begin{aligned} y^{(j)} &= y_1^{(j)} + \cdots + y_{k_0}^{(j)}, \ \ (1 \leqslant j \leqslant 2^\tau) \\ y_i^{(j)} &\in A_{\mu k_0 + i}, \ \ (1 \leqslant i \leqslant k_0). \end{aligned}$$

Ας πούμε, για $\mu = 0$, η (5.3.12) γράφεται ως εξής:

$$\begin{aligned} &\big(y_1^{(1)} + y_2^{(1)} + \cdots + y_{k_0}^{(1)}\big) + \big(y_1^{(2)} + y_2^{(2)} + \cdots + y_{k_0}^{(2)}\big) + \cdots + \big(y_1^{(2^{\tau-1})} + y_2^{(2^{\tau-1})} + \cdots + y_{k_0}^{(2^{\tau-1})}\big) \\ &\quad - \big(y_1^{(2^{\tau-1}+1)} + y_2^{(2^{\tau-1}+1)} + \cdots + y_{k_0}^{(2^{\tau-1}+1)}\big) - \cdots - \big(y_1^{(2^\tau)} + y_2^{(2^\tau)} + \cdots + y_{k_0}^{(2^\tau)}\big) = 0, \end{aligned}$$

ή αλλάζοντας τη σειρά των όρων:

$$\begin{aligned} &\big(y_1^{(1)} + y_1^{(2)} + \cdots + y_1^{(2^{\tau-1})}\big) - \big(y_1^{(2^{\tau-1}+1)} - \cdots - y_1^{(2^\tau)}\big) \\ &+ \big(y_2^{(1)} + y_2^{(2)} + \cdots + y_2^{(2^{\tau-1})}\big) - \big(y_2^{(2^{\tau-1}+1)} - \cdots - y_2^{(2^\tau)}\big) \\ &+ \cdots + \big(y_{k_0}^{(1)} + y_{k_0}^{(2)} + \cdots + y_{k_0}^{(2^{\tau-1})}\big) - \big(y_{k_0}^{(2^{\tau-1}+1)} - \cdots - y_{k_0}^{(2^\tau)}\big), \end{aligned}$$

όπου κάθε $y_i^{(j)}$ εδώ είναι ένας αριθμός της μορφής $h_i\varphi_i(\upsilon_i^{(j)})$, και $|\upsilon_i^{(j)}| \leqslant 2N^{1/k}$. Έτσι η τελευταία εξίσωση μπορεί να γραφτεί ισοδύναμα ως:

$$\begin{aligned} &h_1\Big(\varphi_1(\upsilon_1^{(1)}) + \varphi_1(\upsilon_1^{(2)}) + \cdots + \varphi_1(\upsilon_1^{(2^{\tau-1})}) - \varphi_1(\upsilon_1^{(2^{\tau-1}+1)}) - \cdots - \varphi_1(\upsilon_1^{(2^\tau)})\Big) \\ &+ h_2\Big(\varphi_2(\upsilon_2^{(1)}) + \varphi_2(\upsilon_2^{(2)}) + \cdots + \varphi_2(\upsilon_2^{(2^{\tau-1})}) - \varphi_2(\upsilon_2^{(2^{\tau-1}+1)}) - \cdots - \varphi_2(\upsilon_2^{(2^\tau)})\Big) \\ &\qquad\vdots \\ &+ h_{k_0}\Big(\varphi_{k_0}(\upsilon_{k_0}^{(1)}) + \varphi_{k_0}(\upsilon_{k_0}^{(2)}) + \cdots + \varphi_{k_0}(\upsilon_{k_0}^{(2^{\tau-1})}) - \varphi_{k_0}(\upsilon_{k_0}^{(2^{\tau-1}+1)}) - \cdots - \varphi_{k_0}(\upsilon_{k_0}^{(2^\tau)})\Big). \end{aligned}$$

Θέτοντας για συντομία

$$\varphi_i(\upsilon_i^{(1)}) + \varphi_i(\upsilon_i^{(2)}) + \cdots + \varphi_i(\upsilon_i^{(2^{\tau-1})}) - \varphi_i(\upsilon_i^{(2^{\tau-1}+1)}) - \cdots - \varphi_i(\upsilon_i^{(2^\tau)}) = z_i$$

για $1 \leqslant i \leqslant k_0$, μπορούμε να ξαναγράψουμε την εξίσωση ως

$$h_1 z_1 + h_2 z_2 + \cdots + h_{k_0} z_{k_0} = 0. \tag{5.3.13}$$

Πάντα θα έχουμε 2^τ εξισώσεις αυτής της μορφής, και το σύνολό τους μπορεί να γραφτεί ως

$$\sum_{i=1}^{k_0} h_{\mu k_0 + i} z_{\mu k_0 + i} = 0, \qquad 0 \leqslant \mu \leqslant 2^\tau - 1. \tag{5.3.14}$$

Θα εξετάσουμε το πλήθος των λύσεων της εξίσωσης (5.3.13), καθώς και οι υπόλοιπες συμπεριφέρονται όμοια. Όπως ορίσαμε παραπάνω,

$$\varphi_i(y) = \sum_{u=1}^{k} a_{i,u} y^{k-u},$$

όπου

$$a_{i,u} = \sum_{\upsilon=0}^{u-1} a_\upsilon \binom{k-u}{u-\upsilon} h_i^{u-\upsilon-1}$$

για $i \leqslant s/2$. Αφού έχουμε υποθέσει πως $|a_\upsilon| \leqslant c(k)N^{\upsilon/k}$ και $|h_i| \leqslant 2N^{1/k}$, έχουμε

$$|a_{i,u}| \leqslant \sum_{\upsilon=0}^{u-1} c(k)N^{\frac{\upsilon}{k}} \binom{k-u}{u-\upsilon} c(k)N^{\frac{u-\upsilon-1}{k}} = c(k)N^{\frac{u-1}{k}} \sum_{\upsilon=0}^{u-1} \binom{k-u}{u-\upsilon},$$

και εφόσον $u \leqslant k$, ισχύει ότι

$$\sum_{\upsilon=0}^{u-1} \binom{k-u}{u-\upsilon} \leqslant \sum_{\upsilon=0}^{k} \binom{k-u}{u-\upsilon} \leqslant \sum_{\upsilon=0}^{k} \binom{k}{\upsilon} = 2^k.$$

Έτσι παίρνουμε τελικά ότι

$$|a_{i,u}| \leqslant c(k)N^{\frac{u-1}{k}}.$$

Από την άλλη πλευρά, καθώς $|\upsilon_i^{(j)}| \leqslant 2N^{1/k}$, προκύπτει ότι $|\upsilon_i^{(j)}|^{k-u} \leqslant c(k)N^{(k-u)/k}$ και άρα

$$|a_{i,u}||\upsilon_i^{(j)}| \leqslant c(k)N^{(k-1)/k}.$$

Η ίδια εκτίμηση, με άλλη σταθερά $c(k)$, ισχύει για όλα τα $\varphi_i(\upsilon_i^{(j)})$, καθώς το πλήθος των όρων κάθε τέτοιου πολυωνύμου είναι k. Συνεπώς,

$$|\varphi_i(\upsilon_i^{(j)})| \leqslant c(k)N^{(k-1)/k},$$

για $1 \leqslant i \leqslant k_0$ και $1 \leqslant j \leqslant 2^\tau$. Όμως κάθε z_i είναι το άθροισμα $2^\tau = c(k)$ το πλήθος όρων της μορφής $\pm\varphi_i(\upsilon_i^{(j)})$, και άρα έπεται ότι

$$|z_i| \leqslant c(k)N^{(k-1)/k} \tag{5.3.15}$$

για $1 \leqslant i \leqslant s/2$. Αυτό σημαίνει ότι στην εξίσωση (5.3.14) κάθε z_i μπορεί να πάρει μόνο τιμές εντός του διαστήματος $[-c(k)N^{(k-1)/k}, c(k)N^{(k-1)/k}]$.

Έστω p ένας αριθμός σε αυτό το διάστημα. Τότε η εξίσωση $z_i = p$ μπορεί να ικανοποιηθεί με περισσότερους από έναν τρόπους, καθώς από τον ορισμό του αριθμού z_i, είναι φανερό ότι μπορούμε να έχουμε $z_i = z_j$, με $i \neq j$, από διαφορετικές επιλογές των αριθμών $\upsilon_i^{(j)}$. Οπότε, πρέπει να υπολογίσουμε το πλήθος των λύσεων της εξίσωσης

$$\varphi_i(\upsilon_i^{(1)}) + \varphi_i(\upsilon_i^{(2)}) + \cdots + \varphi_i(\upsilon_i^{(2^{\tau-1})}) - \varphi_i(\upsilon_i^{(2^{\tau-1}+1)}) - \cdots - \varphi_i(\upsilon_i^{(2^\tau)}) = p. \tag{5.3.16}$$

θα χρησιμοποιήσουμε την επαγωγή που κάναμε νωρίτερα.

Αρχικά ξαναγράφουμε την εξίσωση (5.3.16) στη μορφή

$$\varphi_i(v_i^{(1)})+\varphi_i(v_i^{(2)})+\cdots+\varphi_i(v_i^{(s')}) = p-\varphi_i(v_i^{(s'+1)})-\cdots+\varphi_i(v_i^{(2^{\tau-1})})+\cdots+\varphi_i(v_i^{(2^{\tau})}). \tag{5.3.17}$$

Αυτό είναι εφικτό καθώς για $s' = s(k-1) > 1$ (έχουμε δει ήδη ότι $s(1) = 2$) όπως εύκολα μπορούμε να δούμε

$$2^{\tau-1} = 2^{[4\ln_2 s']-2} > s'.$$

Αν γράψουμε το δεξιό μέλος της τελευταίας εξίσωσης ως p', παίρνουμε

$$\varphi_i(v_i^{(1)}) + \varphi_i(v_i^{(2)}) + \cdots + \varphi_i(v_i^{s'}) = p'. \tag{5.3.18}$$

Διαλέγουμε κάποιες συγκεκριμένες τιμές για τους αριθμούς $v_i^{(j)}$, $s'+1 \leqslant j \leqslant 2^\tau$, στο διάστημα $[-2N^{1/k}, 2N^{1/k}]$. Τότε και ο p' παίρνει μία καθορισμένη τιμή. Στην εξίσωση (5.3.18) εφαρμόζουμε την επαγωγική υπόθεση. Το πολυώνυμο $\varphi_i(y)$ είναι ένα πολυώνυμο βαθμού $k-1$. Ελέγχουμε ότι ικανοποιούνται όλες οι απαραίτητες υποθέσεις: Έχουμε

$$\varphi_i(y) = \sum_{u=1}^{k} a_{i,u} y^{k-u},$$

και

$$|a_{i,u}| \leqslant c(k)N^{\frac{u-1}{k}} = c(k)\big(N^{\frac{k-1}{k}}\big)^{\frac{u-1}{k-1}}, \tag{5.3.19}$$

και όπως εύκολα βλέπουμε,

$$p' \leqslant c(k)N^{\frac{k-1}{k}},$$

αφού το p και όλα τα $\varphi_i(y_i^{(j)})$ ικανοποιούν την ανισότητα αυτή.

Από την προηγούμενη ανισότητα, βλέπουμε ότι το $c(k)N^{\frac{k-1}{k}}$ παίρνει το ρόλο του N. Έτσι οι συνθήκες για τα $a_{i,u}$, τις οποίες ικανοποιεί το πολυώνυμο $\varphi_i(y)$, είναι ακριβώς οι συνθήκες της (5.3.7) με $k-1$ στη θέση του k. Βλέπουμε λοιπόν ότι όλες οι υποθέσεις πληρούνται και συνεπώς μπορούμε να υποθέσουμε ότι το πλήθος των λύσεων της εξίσωσης (5.3.18), για τις οποίες

$$v_i^{(j)} \leqslant 2N^{1/k} = 2(N^{\frac{k-1}{k}})^{\frac{1}{k-1}},$$

δεν ξεπερνά τον αριθμό

$$c(k)\big(N^{\frac{k-1}{k}}\big)^{\frac{s'}{k-1}-1} = c(k)N^{\frac{s'-k+1}{k}}. \tag{5.3.20}$$

Αυτή η εκτίμηση έγινε για τις σταθεροποιημένες τιμές $v_i^{(s'+1)}, \ldots, v_i^{(2^\tau)}$. Προφανώς, έχουμε το πολύ

$$(4N^{\frac{1}{k}}+1)^{2^\tau-s'} \leqslant c(k)N^{\frac{2^\tau-s'}{k}} \tag{5.3.21}$$

επιλογές για τα $v_i^{(s'+1)}, \ldots, v_i^{(2^\tau)}$. Το συνολικό πλήθος λύσεων της (5.3.17) έχει ένα άνω φράγμα το οποίο το βρίσκουμε πολλαπλασιάζοντας τα δεξιά μέλη των (5.3.20) και (5.3.21). Έτσι έχουμε το άνω φράγμα

$$c(k)N^{\frac{2^\tau-k+1}{k}}. \tag{5.3.22}$$

Επιστρέφουμε στην εξίσωση (5.3.13). Όπως είδαμε μπορούμε να υποθέσουμε ότι κάθε αριθμός z_i παίρνει τιμές μόνο στο διάστημα $[-c(k)N^{(k-1)/k}, c(k)N^{(k-1)/k}]$. Τώρα είδαμε επιπλέον ότι και η πολλαπλότητα κάθε μίας από αυτές τις τιμές δεν ξεπερνά το άνω φράγμα (5.3.22).

Αυτό το αποτέλεσμα κάνει δυνατή την αναγωγή όλου του προβλήματος σε μια εκτίμηση πλήθους λύσεων γραμμικών εξισώσεων.

Όλοι οι παραπάνω υπολογισμοί έγιναν υπό την υπόθεση ότι οι αριθμοί h_i μας έχουν δοθεί και είναι σταθεροποιημένοι. Άρα οφείλουμε να πολλαπλασιάσουμε το αποτέλεσμα το οποίο έχουμε με τον αριθμό όλων των δυνατών επιλογών για τους αριθμούς αυτούς.

Πριν προχωρήσουμε σε αυτήν την κατεύθυνση ας συνοψίσουμε τι έχουμε καταφέρει ως τώρα:

Ο αριθμός $r_{k,s}^{(f)}(m)$, δεν ξεπερνά το άθροισμα του πλήθους των λύσεων στους ακέραιους z_i με $|z_i| \leqslant c(k)N^{(k-1)/k}$ και αντίστοιχες πολλαπλότητες $\ell_i \leqslant c(k)N^{\frac{2^\tau-k+1}{k}}$, των εξισώσεων της μορφής

$$\sum_{i=1}^{k_0} h_{\mu k_0+i} z_{\mu k_0+i} = 0 \tag{5.3.23}$$

όπου ο αριθμός μ παίρνει τις τιμές $0, 1, \dots, 2^\tau - 1$ και οι h_r, για $1 \leqslant r \leqslant 2^\tau k_0$, ανεξάρτητα ο ένας από τον άλλον, παίρνουν τιμές στο διάστημα $[-2N^{1/k}, 2N^{1/k}]$.

Τώρα έχουμε αναγάγει το πρόβλημα σε μια εκτίμηση του πλήθους των λύσεων γραμμικών εξισώσεων που είναι ανεξάρτητες από τη συγκεκριμένη μορφή του πολυωνύμου $f(x)$, και θα εφαρμόσουμε το Λήμμα 5.2.3.

Έστω K ένας οποιοσδήποτε συνδυασμός των αριθμών h_i, όπου $|h_i| \leqslant 2N^{1/k}$ για κάθε $1 \leqslant i \leqslant s/2$. Έστω επίσης $U_\mu(K)$ το πλήθος των λύσεων της εξίσωσης (5.3.23), έχοντας υπόψιν το γεγονός ότι οι λύσεις z_i ικανοποιούν την σχέση $|z_i| \leqslant c(k)N^{(k-1)/k}$ και τα z_i εμφανίζονται με πολλαπλότητες $\ell_i \leqslant c(k)N^{(2^\tau-k+1)/k}$. Από το αποτέλεσμα του προηγούμενου βήματος, έχουμε

$$r_{k,s}^{(f)}(m) \leqslant \sum_K \Big(\sum_{\mu=0}^{2^\tau-1} U_\mu(K) \Big),$$

όπου η άθροιση γίνεται πάνω από όλους τους δυνατούς συνδυασμούς K των αριθμών h_i. Συνεπώς,

$$r_{k,s}^{(f)}(m) \leqslant \sum_{\mu=0}^{2^\tau-1} \Big(\sum_K U_\mu(K) \Big).$$

Δεν υπάρχει διαφορά σε καμία από τις εξισώσεις της μορφής (5.3.23) για τις διάφορες τιμές του μ, και επιπλέον οι σχετικοί περιορισμοί στις λύσεις είναι ίδιοι. Έτσι, μπορούμε να εστιάσουμε τη μελέτη μας στην εξίσωση που αντιστοιχεί στην τιμή $\mu = 0$ και στο συνδυασμό $U_0(K)$. Έτσι, παίρνουμε το άνω φράγμα

$$r_{k,s}^{(f)}(m) \leqslant 2^\tau \sum_K U_0(K) = c(k) \sum_K U_0(K),$$

όπου $U_0(K)$ είναι το πλήθος των λύσεων της εξίσωσης

$$h_1 z_1 + h_2 z_2 + \cdots + h_{k_0} z_{k_0} \tag{5.3.24}$$

για τον δοσμένο συνδυασμό K των h_i. Εδώ, $|z_i| \leqslant c(k)N^{(k-1)/k}$ και τα z_i εμφανίζονται με πολλαπλότητες $\ell_i \leqslant c(k)N^{(2^\tau-k+1)/k}$. Έστω $U_0^*(K)$ το πλήθος των λύσεων της (5.3.24) με την υπόθεση ότι κάθε τιμή του z_i υπολογίζεται μόνο μία φορά. Προφανώς,

$$U_0(K) \leqslant \Big(c(k)N^{\frac{2^\tau-k+1}{k}}\Big)^{k_0} U_0^*(K)$$

ή, καθώς $k_0 = 2k$,

$$U_0(K) \leqslant c(k)N^{2(2^\tau-k+1)}U_0^*(K),$$

και έτσι

$$r_{k,s}^{(f)}(m) \leqslant c(k)N^{2(2^\tau-k+1)} \sum_K U_0^*(K). \tag{5.3.25}$$

Τώρα κάθε K αντιπροσωπεύει έναν επιτρεπτό συνδυασμό τιμών των αριθμών h_i για $1 \leqslant i \leqslant s/2$. Την ίδια στιγμή, ο αριθμός $U_0^*(K)$ προσδιορίζεται πλήρως από τις τιμές των πρώτων $k_0 = 2k$ τέτοιων αριθμών αφού μόνο αυτοί περιέχονται στην εξίσωση (5.3.24). Έχοντας διαλέξει και σταθεροποιήσει ένα συγκεκριμένο σύστημα K, μπορούμε να προσδιορίσουμε μοναδικά ένα άλλο σύστημα K' τιμών των αριθμών $h_1, h_2, \dots, h_{2k}$. Από την άλλη πλευρά, αν μας δοθεί ένα σύστημα K' τιμών των αριθμών $h_1, h_2, \dots, h_{2k}$, αντιστοιχεί σε παραπάνω από ένα συστήματα K, όσοι και οι τρόποι να συμπληρώσουμε τις $s/2 - 2k$ εναπομείνασες τιμές για τους αριθμούς h_i, $2k \leqslant i \leqslant s/2$. Εφόσον κάθε ένα από τα h_i για $2k \leqslant i \leqslant s/2$ πρέπει να ανήκει στο διάστημα $[-2N^{1/k}, 2N^{1/k}]$, είναι φανερό ότι για κάθε σύστημα K', δεν υπάρχουν περισσότερα από

$$c(k)\big(N^{\frac{1}{k}}\big)^{\frac{s}{2}-2k} = c(k)N^{\frac{s}{2k}-2}$$

συστήματα K που αντιστοιχούν στο K'. Οπότε,

$$\sum_K U_0^*(K) \leqslant c(k)N^{\frac{s}{2k}-2} \sum_{K'} U_0^*(K').$$

Εδώ, ο $U_0^*(K')$ είναι το πλήθος των λύσεων στους ακεραίους z_i, $|z_i| \leqslant c(k)N^{(k-1)/k}$ για $1 \leqslant i \leqslant 2k$ της εξίσωσης (5.3.24) με το δοσμένο σύστημα K' των h_i, $|h_i| \leqslant c(k)N^{1/k}$ για $1 \leqslant i \leqslant 2k$, και το άθροισμα εκτείνεται πάνω από όλα τα συστήματα. Έτσι, από την (5.3.25) παίρνουμε:

$$r_{k,s}^{(f)}(m) \leqslant c(k)N^{2(2^\tau-k+1)}N^{\frac{s}{2k}-2} \sum_{K'} U_0^*(K') = c(k)N^{2(2^{\tau+1}-k)} \sum_{K'} U_0^*(K'). \tag{5.3.26}$$

Θέτουμε $l = 2k$, $A = 2N^{\frac{1}{k}}$, $B = c(k)N^{\frac{k-1}{k}}$ και βλέπουμε ότι οι συνθήκες του Λήμματος 5.2.3 πληρούνται. Άρα βρίσκουμε ότι

$$\sum_{K'} U_0^*(K') = c(k)(AB)^{l-1} = c(k)N^{2k-1}.$$

Από αυτό και από την (5.3.26) έπεται ότι

$$r_{k,s}^{(f)}(m) \leqslant c(k)N^{2(2^{\tau+1}-k)}N^{2k-1} = c(k)N^{2^{\tau+2}-1} = c(k)N^{\frac{s}{k}-1},$$

το οποίο ολοκληρώνει την απόδειξη του λήμματος. □

Μέρος II

Το θεώρημα του Freiman

ΚΕΦΑΛΑΙΟ 6

Αθροίσματα συνόλων

6.1 Βασικές εκτιμήσεις

Ορισμός 6.1.1 (αθροίσματα και διαφορές συνόλων)**.** Έστω A και B υποσύνολα μιας αβελιανής ομάδας G. Ορίζουμε

$$A+B=\{a+b : a\in A, b\in B\} \text{ και } A-B=\{a-b : a\in A, b\in B\}.$$

Εντελώς ανάλογα, αν C είναι ένα τρίτο υποσύνολο της G, θέτουμε

$$A+B+C=\{a+b+c : a\in A, b\in B, c\in C\}$$

και ούτω καθεξής. Αν $A\subseteq G$ και $k,l\in\mathbb{Z}^+$ με $(k,l)\neq(0,0)$ τότε $kA-lA$ είναι το σύνολο όλων των στοιχείων $a_1+\cdots+a_k-(a'_1+\cdots+a'_l)$, όπου $a_i,a'_j\in A$.

Ορισμός 6.1.2 (σταθερά διπλασιασμού)**.** Έστω A πεπερασμένο υποσύνολο της αβελιανής ομάδας G. Η *σταθερά διπλασιασμού* του A είναι η ποσότητα

$$\sigma(A)=\frac{|A+A|}{|A|}.$$

Γενικότερα, αν A,B είναι πεπερασμένα υποσύνολα της G, ορίζουμε

$$\sigma(A,B)=\frac{|A+B|}{\sqrt{|A|\,|B|}}.$$

Θεώρημα 6.1.3 (πρώτη ανισότητα του Ruzsa)**.** *Έστω A,B και C πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Τότε,*

$$|A|\,|B-C|\leqslant|A-B|\,|A-C|. \tag{6.1.1}$$

Απόδειξη. Ορίζουμε απεικόνιση $\varphi : A\times(B-C)\to(A-B)\times(A-C)$ ως εξής: για κάθε $d\in B-C$ επιλέγουμε κάποιο ζευγάρι στοιχείων $b(d)\in B$ και $c(d)\in C$ ώστε $b(d)-c(d)=d$ και θέτουμε

$$\varphi(a,d)=(a-b(d),a-c(d)).$$

Παρατηρούμε ότι η φ είναι 1-1: έστω ότι $\varphi(a,d) = \varphi(a_1,d_1)$. Τότε, $a_1 - b(d_1) = a - b(d)$ και $a_1 - c(d_1) = a - c(d)$. Αφαιρώντας κατά μέλη έχουμε

$$d_1 = b(d_1) - c(d_1) = b(d) - c(d) = d$$

και αυτό σημαίνει ότι $b(d) = b(d_1)$ και $c(d) = c(d_1)$. Έπεται ότι $a_1 = a - b(d) + b(d_1) = a$. Αφού η φ είναι 1-1 έχουμε

$$|A \times (B-C)| \leqslant |(A-B) \times (A-C)|$$

και έπεται το ζητούμενο. □

Διαιρώντας τα δύο μέλη της ανισότητας (6.1.1) με $|A|^2\sqrt{|B|\,|C|}$ και παίρνοντας λογαρίθμους έχουμε την *τριγωνική ανισότητα του Ruzsa*:

Πόρισμα 6.1.4 (τριγωνική ανισότητα)**.** *Έστω A, B και C πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Τότε,*

$$\log \frac{|B-C|}{\sqrt{|B|\,|C|}} \leqslant \log \frac{|A-B|}{\sqrt{|A|\,|B|}} + \log \frac{|A-C|}{\sqrt{|A|\,|C|}}. \tag{6.1.2}$$

Ορισμός 6.1.5 (απόσταση Ruzsa)**.** Αν A και B είναι πεπερασμένα υποσύνολα της αβελιανής ομάδας G, η *απόσταση Ruzsa* των A και B είναι η ποσότητα

$$d(A,B) = \log \frac{|A-B|}{\sqrt{|A|\,|B|}}.$$

Παρατηρήστε ότι

$$|A-B| \geqslant \max\{|A|,|B|\} \geqslant \sqrt{|A|\,|B|},$$

συνεπώς $d(A,B) \geqslant 0$. Επίσης, είναι φανερό ότι $d(A,B) = d(B,A)$ και $d(A+x, B+y) = d(A,B)$ για κάθε $x, y \in G$. Η ανισότητα του Ruzsa εξασφαλίζει την τριγωνική ανισότητα γι' αυτή την απόσταση. Παρατηρήστε όμως ότι η d δεν είναι μετρική: (α) μπορεί να συμβεί να ισχύει $d(A,B) = 0$ για κάποια $A \neq B$ και (β) δεν είναι γενικά σωστό ότι $d(A,A) = 0$.

Σημείωση 6.1.6. Απλή εφαρμογή της τριγωνικής ανισότητας είναι η

$$d(A,A) \leqslant d(A,B) + d(B,A) = 2d(A,B).$$

Αν το A είναι «κοντά» σε κάποιο B τότε, αναγκαστικά, το A είναι «κοντά» στο A. Η ανισότητα αυτή γράφεται και στη μορφή

$$|B|\,|A-A| \leqslant |A \pm B|^2.$$

Ειδικότερα,

$$d(A,A) \leqslant 2d(A,-A).$$

6.2 Προσθετική ενέργεια

Ορισμός 6.2.1 (προσθετική ενέργεια)**.** Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Η *προσθετική ενέργεια* των A και B είναι η ποσότητα

$$\begin{aligned} E(A,B) &= |\{(a,a_1,b,b_1) \in A\times A\times B\times B : a+b=a_1+b_1\}| \\ &= |\{(a,a_1,b,b_1) \in A\times A\times B\times B : a-b_1=a_1-b\}| \\ &= |\{(a,a_1,b,b_1) \in A\times A\times B\times B : a-a_1=b_1-b\}|. \end{aligned}$$

Παρατηρήστε ότι

$$E(A,B) = E(B,A) = E(A,-B)$$

και

$$E(A+x,B+y) = E(A,B), \quad x,y\in G.$$

Απλές εκτιμήσεις που προκύπτουν άμεσα από τον ορισμό είναι οι

$$|A|\,|B| \leqslant E(A,B) \leqslant \min\{|A|^2|B|, |B|^2|A|\}. \tag{6.2.1}$$

Η αριστερή ανισότητα προκύπτει από την παρατήρηση ότι $a+b=a+b$ για κάθε $a\in A, b\in B$. Η ανισότητα $E(A,B)\leqslant |A|^2|B|$ προκύπτει από την παρατήρηση ότι, για κάθε $a,a_1\in A, b\in B$ υπάρχει το πολύ ένα $b_1\in B$ ώστε $a+b=a_1+b_1$ (το $b_1=a+b-a_1$ μπορεί να ανήκει ή να μην ανήκει στο B). Με τον ίδιο τρόπο βλέπουμε ότι $E(A,B)\leqslant |B|^2|A|$.

Ορισμός 6.2.2. Για κάθε $x\in G$ συμβολίζουμε με $s(x)$ το πλήθος των ζευγαριών $(a,b)\in A\times B$ για τα οποία $x=a+b$ και για κάθε $y\in G$ συμβολίζουμε με $r(y)$ το πλήθος των ζευγαριών $(a,b)\in A\times B$ για τα οποία $y=a-b$. Με άλλα λόγια,

$$s(x) = |A\cap (x-B)| \text{ και } r(y) = |A\cap (y+B)|.$$

Πρόταση 6.2.3 (βασικές ταυτότητες)**.** *Ισχύουν οι ισότητες*

$$E(A,B) = \sum_{x\in G} s(x)^2 = \sum_{x\in G} r(y)^2 = \sum_{z\in G} |A\cap (z+A)|\,|B\cap (z+B)| \tag{6.2.2}$$

και

$$|A|\,|B| = \sum_{y\in A-B} r(y) = \sum_{x\in A+B} s(x). \tag{6.2.3}$$

Απόδειξη. Για την πρώτη ισότητα στην (6.2.2) παρατηρούμε ότι

$$\begin{aligned} \sum_{x\in A+B} s(x)^2 &= \sum_{x\in A+B} |A\cap (x-B)|^2 \\ &= \sum_{x\in A+B} |\{(a,b)\in A\times B : a+b=x\}|^2 \\ &= \sum_{x\in A+B} |\{(a,a_1,b,b_1)\in A\times A\times B\times B : a+b=a_1+b_1=x\}| \\ &= E(A,B). \end{aligned}$$

Οι άλλες δύο ισότητες προκύπτουν με τον ίδιο τρόπο: αρκεί να παρατηρήσουμε ότι οι $a+b = a_1+b_1$, $a - b_1 = a_1 - b$ και $a - a_1 = b_1 - b$ είναι ισοδύναμες.

Για την πρώτη ισότητα στην (6.2.3) παρατηρούμε ότι

$$|A|\,|B| = \sum_{(a,b)\in A\times B} 1 = \sum_{x\in G}\ \sum_{\{(a,b)\in A\times B:\, x=a+b\}} 1 = \sum_{x\in G} s(x).$$

Η άλλη ισότητα αποδεικνύεται με τον ίδιο τρόπο. □

Πρόταση 6.2.4 (βασικές ανισότητες)**.** *Έστω A, B πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Τότε,*

(i) $E(A,B) \leqslant |A|\,|B|\,\max(s)$.

(ii) $E(A,B) \leqslant |A|\,|B|\,\max(r)$.

(iii) $|A|^2|B|^2 \leqslant |A+B|\,E(A,B)$.

(iv) $|A|^2|B|^2 \leqslant |A-B|\,E(A,B)$.

(v) $E(A,B) \leqslant \sqrt{E(A,A)\,E(B,B)}$.

Απόδειξη. Για την πρώτη ανισότητα παρατηρούμε ότι, από τις βασικές ταυτότητες της προηγούμενης πρότασης,

$$E(A,B) = \sum_{x\in A+B} s(x)^2 \leqslant \left(\sum_{x\in A+B} s(x)\right)\max(s) = |A|\,|B|\,\max(s).$$

Η δεύτερη ανισότητα αποδεικνύεται με τον ίδιο τρόπο:

$$E(A,B) = \sum_{y\in A-B} r(y)^2 \leqslant \left(\sum_{y\in A-B} r(y)\right)\max(r) = |A|\,|B|\,\max(r).$$

Η τρίτη ανισότητα είναι συνέπεια της ανισότητας Cauchy–Schwarz:

$$|A|^2|B|^2 = \left(\sum_{x\in A+B} s(x)\right)^2 \leqslant |A+B| \sum_{x\in A+B} s(x)^2 = |A+B|\,E(A,B),$$

ενώ η τέταρτη ανισότητα αποδεικνύεται με τον ίδιο τρόπο. Τέλος, η πέμπτη ανισότητα προκύπτει αν εφαρμόσουμε την ανισότητα Cauchy–Schwarz στην

$$E(A,B)^2 = \sum_{z\in G} |A\cap(z+A)|\,|B\cap(z+B)|.$$

□

Θεώρημα 6.2.5 (δεύτερη ανισότητα του Ruzsa)**.** *Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Τότε,*

$$d(A,-B) \leqslant 3d(A,B). \tag{6.2.4}$$

Θα χρησιμοποιήσουμε το ακόλουθο λήμμα:

Λήμμα 6.2.6. *Για κάθε $x \in A+B$ ισχύει*

$$s(x) \leqslant \frac{|A-B|^2}{|A+B|}.$$

Απόδειξη. Έστω $x \in A+B$. Ορίζουμε $D = \{(a,b) \in A \times B : a+b = x\}$. Ορίζουμε απεικόνιση $\psi : D \times (A+B) \to (A-B) \times (A-B)$ ως εξής: για κάθε $y \in A+B$ επιλέγουμε κάποιο ζευγάρι στοιχείων $a(y) \in A$ και $b(y) \in B$ ώστε $y = a(y)+b(y)$ και θέτουμε

$$\psi((a,b),y) = (a-b(y), a(y)-b).$$

Παρατηρούμε ότι η ψ είναι 1-1: ας υποθέσουμε ότι $\psi((a,b),y) = \psi((a_1,b_1),y_1)$. Τότε, ισχύουν οι ισότητες

$$a+b = a_1+b_1 = x_0, \quad a-b(y) = a_1-b(y_1), \quad a(y)-b = a(y_1)-b_1.$$

Έπεται ότι

$$\begin{aligned} y &= a(y)+b(y) = a+b-(a-b(y))+(a(y)-b) \\ &= a_1+b_1-(a_1-b(y_1))+(a(y_1)-b_1) = a(y_1)+b(y_1) \\ &= y_1. \end{aligned}$$

Συνεπώς, $a(y) = a(y_1)$ και $b(y) = b(y_1)$, απ' όπου βλέπουμε ότι $a = a_1$ και $b = b_1$. Αφού η ψ είναι 1-1, έχουμε $|D|\,|A+B| \leqslant |A-B|^2$. □

Απόδειξη του Θεωρήματος 6.2.5. Από την Πρόταση 6.2.4 και το Λήμμα 6.2.6 έχουμε

$$E(A,B) \leqslant |A|\,|B|\,\max(s) \leqslant |A|\,|B|\,\frac{|A-B|^2}{|A+B|}.$$

Πάλι από την Πρόταση 6.2.4,

$$|A|^2|B|^2 \leqslant |A-B|\,E(A,B).$$

Συνδυάζοντας τις δύο ανισότητες βλέπουμε ότι

$$|A+B| \leqslant \frac{|A-B|^3}{|A|\,|B|}.$$

Διαιρώντας με $\sqrt{|A|\,|B|}$ και παίρνοντας λογαρίθμους, συμπεραίνουμε ότι $d(A,-B) \leqslant 3d(A,B)$. □

Σημείωση 6.2.7. Θέτοντας B όπου $-B$ βλέπουμε ότι ισχύει και η $d(A,B) \leqslant 3d(A,-B)$.

6.3 Λογισμός του Ruzsa

Στη συνέχεια χρησιμοποιούμε την εξής σύμβαση για το συμβολισμό: σταθεροποιούμε μια σταθερά $K \geqslant 2$ και γράφοντας $X \lessapprox Y$ εννοούμε ότι $X \leqslant K^c Y$ όπου $c > 0$ απόλυτη σταθερά. Γράφουμε $X \approx Y$ αν $X \lessapprox Y$ και $Y \lessapprox X$. Η τάξη μεγέθους της σταθεράς K θα διευκρινίζεται όταν αυτό έχει σημασία.

Συνδυάζοντας τις δύο ανισότητες του Ruzsa μπορούμε συχνά να ελέγχουμε την απόσταση δύο συνόλων $A, B \subset G$. Γράφουμε $A \sim B$ αν

$$\frac{|A-B|}{\sqrt{|A|\,|B|}} \approx 1.$$

Από την $|A-B| \geqslant \sqrt{|A|\,|B|}$ έπεται ότι για την $A \sim B$ αρκεί να ισχύει η $|A-B| \lessapprox \sqrt{|A|\,|B||}$. Παρατηρήστε επίσης ότι δεν ισχύει απαραίτητα $A \sim A$ (αυτό ισχύει αν $\sigma(A) \approx 1$).

Θεώρημα 6.3.1 (λογισμός του Ruzsa)**.** *Έστω A, B και C υποσύνολα της αβελιανής ομάδας G.*

(i) *Αν $A \sim B$ τότε $A \sim -B$ και $|A| \approx |B|$.*

(ii) *Αν $A \sim B$ και $B \sim C$ τότε $A \sim C$.*

(iii) *Αν $A \sim B$ τότε $\sigma(A) \approx 1$ και $\sigma(B) \approx 1$.*

(iv) *Αν $A \sim B$, $\sigma(C) \approx 1$ και υπάρχει $x \in G$ ώστε $|A \cap (x+C)| \approx |A| \approx |C|$, τότε $A \sim B \sim C$.*

(v) *Αν $\sigma(A), \sigma(C) \approx 1$ και υπάρχει $x \in G$ ώστε $|A \cap (x+C)| \approx |A| \approx |C|$, τότε $A \sim C$.*

Απόδειξη. (i) Από την $A \sim B$ έχουμε

$$\max\{|A|, |B|\} \leqslant |A-B| \lessapprox \sqrt{|A|\,|B|}, \tag{6.3.1}$$

άρα $|A| \lessapprox |B|$ και $|B| \lessapprox |A|$. Συνεπώς, $|A| \approx |B|$. Από τη δεύτερη ανισότητα του Ruzsa, $d(A,-B) \leqslant 3d(A,B)$ και από την $A \sim B$ έπεται ότι

$$|A+B| \leqslant \frac{|A-B|^3}{|A|\,|B|} \lessapprox \sqrt{|A|\,|B|},$$

συνεπώς $A \sim -B$.

(ii) Από την τριγωνική ανισότητα για την d και τις $A \sim B$, $B \sim C$ έχουμε

$$\frac{|A-C|}{\sqrt{|A|\,|C|}} \leqslant \frac{|A-B|}{\sqrt{|A|\,|B|}}\,\frac{|B-C|}{\sqrt{|B|\,|C|}} \lessapprox 1. \tag{6.3.2}$$

Συνεπώς, $A \sim C$.

(iii) Από την $A \sim B$ και το (i) έπεται ότι $B \sim -A$. Τότε, από το (ii) έχουμε $A \sim -A$. Δηλαδή, $|A+A| \approx |A|$. Ισοδύναμα, $\sigma(A) \approx 1$ (και, όμοια, $\sigma(B) \approx 1$).

(iv) Μπορούμε να υποθέσουμε ότι $x = 0$ (αντικαθιστώντας το C με το $x+C$). Από την πρώτη ανισότητα του Ruzsa, χρησιμοποιώντας και τις $A \cap C \subseteq A, C$, παίρνουμε

$$|A \cap C|\,|A-C| \leqslant |(A \cap C) - A|\,|(A \cap C) - C| \leqslant |A-A|\,|C-C|. \tag{6.3.3}$$

Από το (iii) έχουμε $A \sim A$, δηλαδή $|A-A| \approx |A|$. Όμοια, από την υπόθεση έχουμε $\sigma(C) \approx 1$, άρα $C \sim -C$. Από το (i) έπεται ότι $C \sim C$, δηλαδή $|C-C| \approx |C|$. Έτσι, η (6.3.3) παίρνει τη μορφή

$$|A \cap C|\,|A-C| \lessapprox |A|\,|C|. \tag{6.3.4}$$

Από την υπόθεση έχουμε $|A \cap C| \approx |A| \approx |C|$, οπότε η (6.3.4) μας δίνει

$$|A-C| \approx |A| \approx |C|. \tag{6.3.5}$$

Αυτό αποδεικνύει ότι $A \sim C$ και ο ισχυρισμός έπεται από το (ii) και την $A \sim B$.
(v) Είναι ειδική περίπτωση του (iv): θέτουμε $B = A$. □

Θεώρημα 6.3.2 (ανισότητα τριπλού αθροίσματος)**.** *Έστω A, B και C πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Αν*

$$\max\{d(A,B), d(B,C), d(A,C)\} \leqslant \log K, \tag{6.3.6}$$

τότε

$$|A+B+C| \leqslant K^c \sqrt[3]{|A|}\,\sqrt[3]{|B|}\,\sqrt[3]{|C|}. \tag{6.3.7}$$

Η απόδειξη βασίζεται στην ειδική περίπτωση $n=1$ του ακόλουθου Λήμματος:

Λήμμα 6.3.3. *Υπάρχει σύνολο $S \subseteq A+B$ ώστε*

$$|S| \geqslant \frac{\max\{|A|,|B|\}}{2} \tag{6.3.8}$$

και

$$|A+B+nS| \leqslant \frac{2^n |A+B|^{2n+1}}{|A|^n |B|^n} \tag{6.3.9}$$

για κάθε $n \in \mathbb{N}$.

Απόδειξη. Ορίζουμε

$$S = \left\{ x \in A+B : s(x) \geqslant \frac{|A|\,|B|}{2|A+B|} \right\}. \tag{6.3.10}$$

Τότε,

$$\sum_{x \in [(A+B)\setminus S]} s(x) \leqslant |A+B|\,\frac{|A|\,|B|}{2|A+B|} = \frac{|A|\,|B|}{2} = \frac{1}{2}\sum_{x \in A+B} s(x),$$

άρα

$$\sum_{x \in S} s(x) \geqslant \frac{1}{2}\sum_{x \in A+B} s(x) = \frac{|A|\,|B|}{2}.$$

Αφού $s(x) \leqslant \min\{|A|,|B|\}$, έπεται ότι

$$|S| \geqslant \frac{\max\{|A|,|B|\}}{2}. \tag{6.3.11}$$

Έστω $w \in A+B+nS$. Τότε, υπάρχουν $a_0 \in A$, $s_1, \dots, s_n \in S$, $b_{n+1} \in B$ ώστε $w = a_0 + s_1 + \cdots + s_n + b_{n+1}$. Κάθε s_k γράφεται με τουλάχιστον $\frac{|A|\,|B|}{2|A+B|}$ τρόπους στη μορφή $s_k = b_k + a_k$, όπου $a_k \in A$, $b_k \in B$. Συνεπώς, το w έχει τουλάχιστον $\left(\frac{|A|\,|B|}{2|A+B|}\right)^n$ αναπαραστάσεις της μορφής

$$w = a_0 + (b_1 + a_1) + \cdots + (b_n + a_n) + b_{n+1} = (a_0 + b_1) + (a_1 + b_2) + \cdots + (a_n + b_{n+1}).$$

Αν σταθεροποιήσουμε τα $a_0, s_1, \dots, s_n, b_{n+1}$ τότε η $(n+1)$-άδα $(a_0+b_1, \dots, a_n+b_{n+1}) \in (A+B)^{n+1}$ προσδιορίζει πλήρως τα a_k, b_k. Δηλαδή, σε κάθε $w \in A+B+nS$ αντιστοιχεί ένα υποσύνολο $T(w)$ του $(A+B)^{n+1}$ με τουλάχιστον $\left(\frac{|A|\,|B|}{2|A+B|}\right)^n$ στοιχεία. Επιπλέον, αν $w \neq w'$ στο $A+B+nS$, τότε $T(w) \cap T(w') = \emptyset$ (το άθροισμα των όρων κάθε $(n+1)$-άδας από το $T(w)$ είναι ίσο με w). Έπεται ότι

$$|A+B|^{n+1} \geqslant \left(\frac{|A|\,|B|}{2|A+B|}\right)^n |A+B+nS|,$$

απ' όπου προκύπτει η (6.3.9). □

Απόδειξη του Θεωρήματος 6.3.2. Από την υπόθεση και από το λογισμό του Ruzsa βλέπουμε ότι

$$|A| \approx |B| \approx |C| \approx |A \pm B| \approx |A \pm C| \approx |B \pm C|.$$

Ειδικότερα, για το θεώρημα αρκεί να δείξουμε ότι

$$|A+B+C| \leqslant K^c |A|.$$

Από το Λήμμα 6.3.3 (με $n=1$) υπάρχει $S \subseteq A+B$ ώστε

$$|A| \lessapprox |S| \text{ και } |A+B+S| \leqslant \frac{2|A+B|^3}{|A|\,|B|},$$

άρα

$$|A+B+S| \lessapprox \sqrt{|A+B|\,|S|}.$$

Συνεπώς, $A+B \sim S$. Από το λογισμό του Ruzsa (μέρος (iii)) έχουμε $\sigma(A+B) \approx 1$.

Από την $d(A,C) \leqslant \log K$ έχουμε $|A-C| \approx |A| \approx |C|$. Αν $r(x)$ είναι το πλήθος των ζευγαριών $(a,c) \in A \times C$ για τα οποία $x = a-c$, έχουμε $r(x) = |A \cap (x+C)|$. Όμως,

$$\sum_{x \in G} r(x) = |A|\,|C|,$$

άρα υπάρχει $x \in A-C$ ώστε $r(x) \gtrapprox |A|$. Θέτοντας $x_1 = x+b$ για κάποιο $b \in B$, παίρνουμε

$$|(A+B) \cap (x_1+C)| \gtrapprox |A|.$$

Από τον ισχυρισμό (iv) του θεωρήματος 6.3.1 έπεται ότι $\sigma(C) \approx 1$. Τότε, από τον ισχυρισμό (v) του θεωρήματος 6.3.1 βλέπουμε ότι $C \sim A+B$. Τότε, $A+B \sim -C$, άρα

$$|A+B+C| \lessapprox \sqrt{|A+B|\,|C|} \approx |A|.$$

□

Πόρισμα 6.3.4 (ανισότητα πολλαπλού αθροίσματος)**.** *Έστω A πεπερασμένο υποσύνολο της αβελιανής ομάδας G με $\sigma(A) \leqslant K$ και έστω $k, l \in \mathbb{Z}^+$ με $(k,l) \neq (0,0)$. Υπάρχει σταθερά $\gamma(k,l)$ ώστε*

$$|kA - lA| \ll K^{\gamma(k,l)}|A|.$$

Το πόρισμα προκύπτει με διαδοχικές εφαρμογές του θεωρήματος. Σε επόμενο κεφάλαιο θα δούμε την απόδειξη μιας πολύ ισχυρότερης εκδοχής του.

6.4 Λήμματα κάλυψης

Τα *λήμματα κάλυψης* που αποδεικνύονται παρακάτω, δείχνουν ότι αν δύο σύνολα $A, B \subseteq G$ έχουν μικρή απόσταση τότε το ένα καλύπτεται από περιορισμένο αριθμό μεταφορών του άλλου (ή κάποιου υποσυνόλου του).

Λήμμα 6.4.1 (λήμμα κάλυψης του Ruzsa)**.** *Έστω $A, B \subseteq G$. Υπάρχει $X \subseteq B$ ώστε*

$$B \subseteq A - A + X, \qquad |X| \leqslant \frac{|A+B|}{|A|}, \qquad |A + X| = |A| \cdot |X|.$$

Όμοια, υπάρχει $Y \subseteq B$ ώστε

$$B \subseteq A - A + Y, \qquad |Y| \leqslant \frac{|A-B|}{|A|}, \qquad |A - Y| = |A| \cdot |Y|.$$

Απόδειξη. Θεωρούμε την οικογένεια $\{A + b : b \in B\}$. Για κάθε $b \in B$, το σύνολο $A + b$ έχει $|A|$ στοιχεία και περιέχεται στο $|A + B|$. Αν πάρουμε μια μεγιστική υποοικογένεια $\{A + x : x \in X\}$ ξένων ανά δύο συνόλων αυτής της μορφής, τότε ισχύουν τα εξής:

(i) Αφού τα $A + x$, $x \in X$ είναι ξένα, έχουμε

$$|A + X| = \left|\bigcup_{x\in X}(A + x)\right| = \sum_{x\in X}|A + x| = |A| \cdot |X|.$$

(ii) Αφού κάθε $A + x \subseteq A + B$, έχουμε

$$|X| \cdot |A| \leqslant |A + B|.$$

(iii) Για κάθε $b \in B$ υπάρχει $x \in X$ ώστε $(A + b) \cap (A + x) \neq \emptyset$, δηλαδή

$$b \in A - A + x \subseteq A - A + X.$$

Άρα, $B \subseteq A - A + X$.

Για τον δεύτερο ισχυρισμό, δουλεύουμε με το $-B$ στη θέση του B. □

Πόρισμα 6.4.2. *Έστω $A, B \subseteq G$. Αν $N(B, A - A)$ είναι ο ελάχιστος αριθμός μεταφορών του $A - A$ που η ένωσή τους καλύπτει το B, έχουμε*

$$N(B, A - A) \leqslant \min\left\{\frac{|A+B|}{|A|}, \frac{|A-B|}{|A|}\right\}.$$

Λήμμα 6.4.3 (λήμμα κάλυψης των Green–Ruzsa)**.** *Έστω $A, B \subseteq G$. Υπάρχει $X \subseteq B$ με πληθάριθμο*

$$|X| \leqslant \frac{2|A+B|}{|A|} - 1,$$

το οποίο ικανοποιεί το εξής: «για κάθε $b \in B$ υπάρχουν τουλάχιστον $|A|/2$ τριάδες $(x, a, a') \in X \times A \times A$ ώστε $b = x + a - a'$». Επιπλέον, έχουμε

$$B - B \subseteq A - A + X - X.$$

Απόδειξη. Θέτουμε $X_0 = \emptyset$. Τότε, $X_0 + A - A = \emptyset$. Αν έχει οριστεί το X_{j-1}, επιλέγουμε $b_j \in B$ με την ιδιότητα

$$|(b_j + A) \cap (X_{j-1} + A)| \leqslant \frac{|A|}{2}$$

και θέτουμε $X_j = X_{j-1} \cup \{b_j\}$. Αν δεν υπάρχει τέτοιο b_j σταματάμε τη διαδικασία. Παρατηρήστε ότι $|X_1 + A| = |A|$ και $|X_j + A| \geqslant |X_{j-1} + A| + |A|/2$. Συνεπώς,

$$|X_j| \geqslant |A| + \frac{j-1}{2}|A| = \frac{j+1}{2}|A|.$$

Ας υποθέσουμε ότι $X = X_k$ είναι το τελικό σύνολο που προκύπτει με αυτόν τον τρόπο. Αφού $A + X \subseteq A + B$, έχουμε

$$\frac{k+1}{2}|A| \leqslant |A+B|,$$

δηλαδή

$$|X| = k \leqslant \frac{2|A+B|}{|A|} - 1.$$

Έστω $b \in B$. Από τον τρόπο ορισμού του X έχουμε $|(A+b) \cap (X+A)| > |A|/2$. Συνεπώς, το b έχει τουλάχιστον $|A|/2$ αναπαραστάσεις της μορφής $b = x+a-a'$ για κάποια τριάδα $(x, a, a') \in X \times A \times A$.

Για τον τελευταίο ισχυρισμό, θεωρούμε $b_1, b_2 \in B$. Τότε,

$$|\{a \in A : b_1 + a \in X + A\}| = |(A + b_1) \cap (X + A)| > \frac{|A|}{2}$$

και

$$|\{a \in A : b_2 + a \in X + A\}| = |(A + b_1) \cap (X + A)| > \frac{|A|}{2}.$$

Άρα, υπάρχει $a \in A$ ώστε $b_1 + a \in X + A$ και $b_2 + a \in X + A$. Τότε,

$$b_1 - b_2 = (b_1 + a) - (b_2 + a) \in (X + A) - (X + A) = A - A + X - X.$$

Δηλαδή, $B - B \subseteq A - A + X - X$. □

Σημείωση 6.4.4. Το λήμμα των Green–Ruzsa μπορεί να χρησιμοποιηθεί για εκτιμήσεις του πληθαρίθμου συνόλων της μορφής $kB - kB$ συναρτήσει της απόστασης των A και B. Για παράδειγμα, με χρήση του λήμματος αποδεικνύονται τα εξής:

(i) Αν $A, B \subseteq G$ τότε

$$|2B - 2B| \leqslant \frac{|A+B|^4 |A-A|}{|A|^4}.$$

(ii) Ειδικότερα,

$$|2A - 2A| \leqslant \frac{|A - A|^5}{|A|^4},$$

άρα

$$d(A - A, A - A) \leqslant 4d(A, A)$$

για κάθε $A \subseteq G$.

ΚΕΦΑΛΑΙΟ 7

Γεωμετρία των αριθμών

7.1 Πλέγματα

Ένα υποσύνολο Λ του $\mathbb{R}^n$, $n \geqslant 2$, λέγεται *πλέγμα* αν υπάρχουν γραμμικά ανεξάρτητα διανύσματα $u_1, \dots, u_n \in \mathbb{R}^n$ ώστε

$$\Lambda = \{x \in \mathbb{R}^n : x = m_1 u_1 + \cdots + m_n u_n, m_i \in \mathbb{Z}\}.$$

Τότε λέμε ότι το $\{u_1, \dots, u_n\}$ είναι μια *βάση* του πλέγματος Λ. Ένα πλέγμα μπορεί να έχει περισσότερες από μία βάσεις (για την ακρίβεια, θα δούμε ότι κάθε πλέγμα έχει άπειρες το πλήθος βάσεις). Παρατηρήστε ότι ένα υποσύνολο Λ του $\mathbb{R}^n$ είναι πλέγμα αν και μόνο αν υπάρχει $T \in GL(n)$ ώστε $\Lambda = T(\mathbb{Z}^n)$.

Πρόταση 7.1.1. *Κάθε πλέγμα Λ στον $\mathbb{R}^n$ είναι διακριτή προσθετική υποομάδα του $\mathbb{R}^n$. Δηλαδή, υπάρχει $r > 0$ ώστε $rB_2^n \cap \Lambda = \{0\}$.*

Απόδειξη. Έστω $\Lambda = T(\mathbb{Z}^n)$, $T \in GL(n)$. Αν $x, y \in \Lambda$ τότε $x - y \in \Lambda$, άρα το Λ είναι προσθετική υποομάδα του $\mathbb{R}^n$. Επίσης, αν ορίσουμε $Q = \{x \in \mathbb{R}^n : |x_i| < 1\}$, τότε $\mathbb{Z}^n \cap Q = \{0\}$. Αφού ο T είναι ένα προς ένα,

$$\Lambda \cap T(Q) = T(\mathbb{Z}^n \cap Q) = \{0\}.$$

Όμως το $T(Q)$ είναι ανοικτό υποσύνολο του $\mathbb{R}^n$ και $0 \in T(Q)$, άρα υπάρχει $r > 0$ ώστε $rB_2^n \subset T(Q)$. Έπεται ότι $rB_2^n \cap \Lambda = \{0\}$. □

Άμεσες συνέπειες του ορισμού της διακριτής προσθετικής ομάδας είναι οι εξής:

(i) Αν $rB_2^n \cap \Lambda = \{0\}$, τότε για κάθε $u \in \Lambda$ ισχύει $B(u, r) \cap \Lambda = \{u\}$.

(ii) Για κάθε $R > 0$, η RB_2^n περιέχει πεπερασμένα το πλήθος σημεία του Λ. Πράγματι, αν για κάποιο $R > 0$ υπήρχαν διακεκριμένα $x_n, n \in \mathbb{N}$, σημεία του Λ στην RB_2^n, τότε θα μπορούσαμε να βρούμε συγκλίνουσα υπακολουθία (x_{k_n}) της (x_n). Τότε, για οποιοδήποτε $r > 0$, θα μπορούσαμε να βρούμε $m, n \in \mathbb{N}$ ώστε $0 \neq x_{k_m} - x_{k_n} \in rB_2^n \cap \Lambda$. Δηλαδή, το Λ δεν θα ήταν διακριτή προσθετική υποομάδα του $\mathbb{R}^n$.

Πρόταση 7.1.2. *Ένα υποσύνολο Λ του $\mathbb{R}^n$ είναι πλέγμα αν και μόνο αν περιέχει n γραμμικά ανεξάρτητα διανύσματα και είναι διακριτή προσθετική υποομάδα του $\mathbb{R}^n$.*

Απόδειξη. Η μία κατεύθυνση δίνεται από την Πρόταση 7.1.1. Για την άλλη κατεύθυνση, υποθέτουμε ότι Λ είναι μια διακριτή προσθετική υποομάδα του $\mathbb{R}^n$, που περιέχει τα γραμμικά ανεξάρτητα διανύσματα $x_1, \ldots, x_n$. Θα κατασκευάσουμε μια βάση του Λ, δηλαδή ένα σύνολο $\{u_1, \ldots, u_n\}$ γραμμικά ανεξάρτητων διανυσμάτων στο Λ με την ιδιότητα: κάθε $v \in \Lambda$ γράφεται μονοσήμαντα στη μορφή $v = m_1u_1 + \cdots + m_nu_n$, όπου $m_1, \ldots, m_n \in \mathbb{Z}$.

Τα $u_1, \ldots, u_n$ θα οριστούν διαδοχικά. Στο πρώτο βήμα, θεωρούμε τον μονοδιάστατο υπόχωρο $F_1 = \langle x_1 \rangle$ που παράγεται από το x_1, και επιλέγουμε ως u_1 ένα μη μηδενικό διάνυσμα του $F_1 \cap \Lambda$ που έχει τη μικρότερη δυνατή απόσταση από το 0. Πιό συγκεκριμένα, μπορούμε να πάρουμε $u_1 = tx_1$, όπου $t > 0$ ο μικρότερος δυνατός ώστε $tx_1 \in \Lambda$. Το Λ είναι διακριτό, άρα το ευθύγραμμο τμήμα $[0, x_1]$ θα περιέχει πεπερασμένα το πλήθος σημεία του πλέγματος. Επομένως, το u_1 είναι καλά ορισμένο.

Συνεχίζουμε επαγωγικά: θα δείξουμε ότι για κάθε $k \leqslant n$ μπορούμε να βρούμε $u_1, \ldots, u_k \in \langle x_1, \ldots, x_k \rangle$ ώστε το $\Lambda \cap \langle x_1, \ldots, x_k \rangle$ να παράγεται (με ακέραιους συντελεστές) από τα $u_1, \ldots, u_k$:

$$\Lambda_k := \Lambda \cap \langle x_1, \ldots, x_k \rangle = \{m_1u_1 + \cdots + m_ku_k : m_i \in \mathbb{Z}\}.$$

Με μια τέτοια κατασκευή, τα u_i είναι γραμμικά ανεξάρτητα και, για $k = n$, έχουμε

$$\Lambda = \{x \in \mathbb{R}^n : x = m_1u_1 + \cdots + m_nu_n, m_i \in \mathbb{Z}\},$$

δηλαδή το Λ είναι πλέγμα.

Για την επιλογή του u_{k+1} θεωρούμε το παραλληλεπίπεδο

$$P = \{x = a_1u_1 + \cdots + a_ku_k + bx_{k+1} : 0 \leqslant a_i < 1, 0 < b \leqslant 1\},$$

και επιλέγουμε σαν u_{k+1} ένα στοιχείο του $P \cap \Lambda$ για το οποίο ο συντελεστής b είναι ο ελάχιστος δυνατός. Το σύνολο $P \cap \Lambda$ είναι μη κενό γιατί $x_{k+1} \in P \cap \Lambda$, και έχει πεπερασμένα το πλήθος σημεία (γιατί το Λ είναι διακριτή ομάδα). Άρα, το u_{k+1} είναι καλά ορισμένο.

Τα $u_1, \ldots, u_k$ είναι γραμμικά ανεξάρτητα, και

$$u_{k+1} = \sum_{i=1}^{k} a_iu_i + bx_{k+1}$$

με $b \neq 0$. Αυτό σημαίνει ότι $u_{k+1} \notin \langle u_1, \ldots, u_k \rangle$, άρα τα $u_1, \ldots, u_{k+1}$ είναι γραμμικά ανεξάρτητα. Θα δείξουμε ότι

$$\Lambda_{k+1} := \Lambda \cap \langle x_1, \ldots, x_{k+1} \rangle = \{m_1u_1 + \cdots + m_{k+1}u_{k+1} : m_i \in \mathbb{Z}\}. \tag{7.1.1}$$

Έστω $x \in \Lambda_{k+1}$. Τα $u_1, \ldots, u_{k+1}$ είναι βάση του $\langle x_1, \ldots, x_{k+1} \rangle$, άρα $x = t_1u_1 + \cdots + t_ku_k + t_{k+1}u_{k+1}$ για κάποιους $t_1, \ldots, t_{k+1} \in \mathbb{R}$. Θέτουμε $\{z\} = z - [z]$ το κλασματικό μέρος του z, και θεωρούμε το

$$x' = \{t_1\}u_1 + \cdots + \{t_k\}u_k + \{t_{k+1}\}u_{k+1} \in \Lambda.$$

Τότε,

$$\begin{aligned} x' &= \{t_1\}u_1 + \cdots + \{t_k\}u_k + \{t_{k+1}\}\left(\sum_{i=1}^{k} a_i u_i + b x_{k+1}\right) \\ &= t_1' u_1 + \cdots + t_k' u_k + \{t_{k+1}\} b x_{k+1} \in \Lambda, \end{aligned}$$

άρα, αν $0 < \{t_{k+1}\}$ τότε

$$x'' = \{t_1'\}u_1 + \cdots + \{t_k'\}u_k + \{t_{k+1}\}bx_{k+1} \in \Lambda \cap P,$$

το οποίο είναι άτοπο αφού $\{t_{k+1}\}b < b$. Έπεται ότι $\{t_{k+1}\} = 0$, δηλαδή $t_{k+1} \in \mathbb{Z}$. Τότε όμως,

$$x' = \{t_1\}u_1 + \cdots \{t_k\}u_k \in \Lambda \cap \langle x_1, \ldots, x_k\rangle,$$

και, από την επαγωγική μας υπόθεση, πρέπει να έχουμε $t_1, \ldots, t_k \in \mathbb{Z}$. Αυτό αποδεικνύει την (7.1.1) και, επαγωγικά, το θεώρημα. □

Παρατήρηση 7.1.3. Η απόδειξη της πρότασης δίνει ταυτόχρονα έναν τρόπο με τον οποίο μπορούμε να περνάμε από ένα γραμμικά ανεξάρτητο υποσύνολο $\{x_1, \ldots, x_n\}$ ενός πλέγματος Λ σε βάση $\{u_1, \ldots, u_n\}$ του Λ, με την ιδιότητα

$$\langle u_1, \ldots, u_k\rangle = \langle x_1, \ldots, x_k\rangle, \qquad 1 \leqslant k \leqslant n.$$

7.1.1 Ορίζουσα πλέγματος

Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$ και έστω $u_1, \ldots, u_n$ μια βάση του. Το παραλληλεπίπεδο

$$Q = \Big\{ \sum_{i=1}^{n} a_i u_i : 0 \leqslant a_i < 1 \Big\}$$

λέγεται *θεμελιώδες παραλληλεπίπεδο* του πλέγματος. Ο όγκος $|Q|$ του Q λέγεται *ορίζουσα του πλέγματος* και συμβολίζεται με $\det \Lambda$.

Η επόμενη πρόταση δείχνει ότι ο όγκος του θεμελιώδους παραλληλεπιπέδου είναι ανεξάρτητος από την επιλογή της βάσης.

Πρόταση 7.1.4. *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, και έστω P, Q δύο θεμελιώδη παραλληλεπίπεδα του Λ. Τότε, $|P| = |Q|$.*

Απόδειξη. Έστω $\{u_1, \ldots, u_n\}$ και $\{v_1, \ldots, v_n\}$ οι βάσεις του Λ που ορίζουν τα θεμελιώδη παραλληλεπίπεδα P και Q. Τότε, αν U, V είναι οι πίνακες που έχουν σαν στήλες τα u_i, v_i αντίστοιχα, έχουμε

$$|P| = |\det U|, \quad |Q| = |\det V|.$$

Γράφουμε τα διανύσματα της μιας βάσης συναρτήσει των διανύσματων της άλλης, και έχουμε

$$u_i = \sum_{j=1}^{n} m_{ij} v_j, \quad v_i = \sum_{j=1}^{n} l_{ij} u_j,$$

όπου $M = (m_{ij})$ και $L = (l_{ij})$ πίνακες με ακέραιες συντεταγμένες. Τότε $U = VM^T$ και $V = UL^T$, άρα $ML = I$. Δηλαδή,

$$|\det M| \cdot |\det L| = 1,$$

και αφού $\det M, \det L \in \mathbb{Z}$, παίρνουμε $|\det M| = |\det L| = 1$. Αυτό σημαίνει ότι

$$|P| = |\det U| = |\det M| \cdot |\det V| = |\det V| = |Q|,$$

δηλαδή το ζητούμενο. □

Αφού ο όγκος οποιουδήποτε θεμελιώδους παραλληλεπιπέδου του Λ είναι πάντα ο ίδιος, η ορίζουσα $\det \Lambda$ του Λ ορίζεται καλά. Μπορούμε μάλιστα με τη βοήθειά της να χαρακτηρίσουμε τις βάσεις του Λ: αν Λ είναι ένα πλέγμα στον $\mathbb{R}^n$, και $u_1, \ldots, u_n \in \Lambda$, τότε τα $u_1, \ldots, u_n$ είναι βάση του Λ αν και μόνο αν

$$|\det(u_1, \ldots, u_n)| = \det \Lambda.$$

Η μία κατεύθυνση είναι προφανής από τον ορισμό της $\det \Lambda$. Για την αντίστροφη κατεύθυνση, έστω $u_1, \ldots, u_n \in \Lambda$ με $|\det(u_1, \ldots, u_n)| = \det \Lambda$. Αφού $\det \Lambda > 0$, τα u_i είναι γραμμικά ανεξάρτητα. Θεωρούμε μία βάση V του Λ, και γράφουμε $U = VM^T$ και $V = UL^T$. Η V είναι βάση του πλέγματος και τα u_i ανήκουν στο Λ, άρα ο M έχει ακέραιες συντεταγμένες. Όμως,

$$|\det U| = |\det V| = \det \Lambda$$

από την υπόθεσή μας, άρα $|\det M| = 1$. Αυτό όμως μάς εξασφαλίζει ότι και ο $L = M^{-1}$ είναι ακέραιος πίνακας, διότι τα στοιχεία του είναι της μορφής

$$l_{ij} = \pm \frac{\det M_{ij}}{\det M} \in \mathbb{Z}.$$

(M_{ij} είναι ο πίνακας που προκύπτει από τον M αν «διαγράψουμε» την i-γραμμή και την j-στήλη του.) Αφού $V = UL^T$ και η V είναι βάση του Λ, τα u_i είναι βάση του Λ.

Η επόμενη πρόταση εξασφαλίζει την ύπαρξη πολλών διαφορετικών βάσεων για κάθε πλέγμα Λ στον $\mathbb{R}^n$, $n \geqslant 2$:

Πρόταση 7.1.5. *Αν $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ και ο μέγιστος κοινός διαιρέτης των $x_1, \ldots, x_n$ είναι 1, τότε το x επεκτείνεται σε βάση του $\mathbb{Z}^n$.*

Απόδειξη. Μπορούμε να βρούμε $y_2, \ldots, y_n \in \mathbb{Z}^n$ ώστε τα $x, y_2, \ldots, y_n$ να είναι γραμμικά ανεξάρτητα: αφού $x \neq 0$, υπάρχει $i_0 \leqslant n$ ώστε $x_{i_0} \neq 0$, οπότε μπορούμε να πάρουμε σαν y_j τα διανύσματα e_i, $i \neq i_0$.

Κατόπιν κατασκευάζουμε βάση $\{u_1, \ldots, u_n\}$ όπως στην Πρόταση 7.1.2, ξεκινώντας από τα $x, y_2, \ldots, y_n$. Παρατηρήστε ότι $u_1 = x$, γιατί το x είναι το πλησιέστερο προς το 0 ακέραιο σημείο του $\langle x \rangle$. Εδώ χρησιμοποιείται η υπόθεση ότι οι $x_1, \ldots, x_n$ έχουν μέγιστο κοινό διαιρέτη τη μονάδα. □

Πόρισμα 7.1.6. *Κάθε πλέγμα Λ στον $\mathbb{R}^n$, $n \geqslant 2$, έχει άπειρες το πλήθος διαφορετικές βάσεις.*

Απόδειξη. Αρκεί να εξετάσουμε την περίπτωση $\Lambda = \mathbb{Z}^n$. Υπάρχουν άπειρες το πλήθος n-άδες μη μηδενικών ακεραίων $x_1, \ldots, x_n$ που έχουν μέγιστο κοινό διαιρέτη τη μονάδα. Κάθε μία από αυτές ανήκει σε μια βάση του $\mathbb{Z}^n$, από την Πρόταση 7.1.5. Άρα, το $\mathbb{Z}^n$ έχει άπειρες διαφορετικές βάσεις. □

Το τελευταίο αποτέλεσμα αυτής της παραγράφου δίνει μια σημαντική ιδιότητα του θεμελιώδους παραλληλεπιπέδου (την οποία θα χρησιμοποιήσουμε αρκετές φορές στη συνέχεια):

Πρόταση 7.1.7. *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, $\{u_1, \ldots, u_n\}$ μια βάση του Λ, και $Q = \{a_1u_1 + \cdots + a_nu_n : 0 \leqslant a_i < 1\}$ το αντίστοιχο θεμελιώδες παραλληλεπίπεδο. Τότε,*

$$\mathbb{R}^n = Q \oplus \Lambda.$$

Δηλαδή, οι μεταφορές του Q κατά τα σημεία του Λ, καλύπτουν τον $\mathbb{R}^n$ χωρίς να επικαλύπτονται.

Απόδειξη. Έστω $x \in \mathbb{R}^n$. Τα u_i είναι βάση του $\mathbb{R}^n$, άρα μπορούμε να γράψουμε $x = \sum_{i=1}^n t_iu_i$ για κάποιους $t_i \in \mathbb{R}$. Θεωρούμε τα διανύσματα

$$y = \sum_{i=1}^n \{t_i\}u_i, \quad z = \sum_{i=1}^n [t_i]u_i.$$

Τότε, $z \in \Lambda$, $y \in Q$, και

$$x = y + z \in Q + \Lambda.$$

Κάθε $x \in \mathbb{R}^n$ γράφεται με μοναδικό τρόπο σε αυτή τη μορφή: Αν για κάποιο $x \in \mathbb{R}^n$ είχαμε $x = y + z = y' + z'$ με $y, y' \in Q$, και $z, z' \in \Lambda$, τότε θα είχαμε $y - y' \in \Lambda$, δηλαδή

$$y - y' = \sum_{i=1}^n b_iu_i, \qquad b_i \in \mathbb{Z}.$$

Όμως, $|b_i| = |a_i(y) - a_i(y')| < 1$ διότι $a_i(y), a_i(y') \in [0, 1)$. Έπεται ότι $b_i = 0$ για κάθε $i \leqslant n$. Οπότε $y = y_1$ και $z = z_1$, που αποδεικνύει το ζητούμενο. □

7.1.2 Υποπλέγματα

Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$ και έστω $\Lambda_0 \subseteq \Lambda$. Αν το Λ_0 είναι πλέγμα, τότε λέμε ότι το Λ_0 είναι *υποπλέγμα* του Λ. Αφού το Λ_0 είναι υποομάδα της αβελιανής ομάδας Λ, ορίζεται η ομάδα πηλίκο $\Lambda : \Lambda_0$. Ο πληθάριθμός της λέγεται *δείκτης* του Λ_0 στο Λ, και συμβολίζεται με $|\Lambda : \Lambda_0|$.

Με αυτό το συμβολισμό, αν $|\Lambda : \Lambda_0| = s$, μπορούμε να γράψουμε το πλέγμα Λ σαν ένωση s το πλήθος ξένων συμπλόκων, δηλαδή

$$\Lambda = \bigcup_{i=1}^s (\Lambda_0 + a_i),$$

όπου $a_1, \ldots, a_s \in \Lambda$. Το πρώτο θεώρημα αυτής της παραγράφου υπολογίζει τον δείκτη του υποπλέγματος Λ_0 στο Λ:

Θεώρημα 7.1.8. *Έστω $V = \{v_1, \ldots, v_n\}$ μία βάση του Λ_0. Αν $Q = \{\sum_{i=1}^n a_iv_i : \ 0 \leqslant a_i < 1\}$ είναι το θεμελιώδες παραλληλεπίπεδο του Λ_0 ως προς την V, τότε*

$$|\Lambda : \Lambda_0| = |Q \cap \Lambda|.$$

Απόδειξη. Αν $y_1 \neq y_2 \in Q \cap \Lambda$, τότε $y_1 + \Lambda_0 \neq y_2 + \Lambda_0$. Πράγματι, αν $y_1 + \Lambda_0 = y_2 + \Lambda_0$, τότε το $y_1 - y_2$ είναι μη μηδενικό και ανήκει στο Λ_0. Επίσης, $y_1 - y_2 \in \{\sum_{i=1}^{n} a_i v_i : \ |a_i| < 1\}$, διότι $y_1, y_2 \in Q$. Όμως, το μοναδικό σημείο του Λ_0 που έχει αυτή την ιδιότητα είναι το μηδενικό. Έπεται ότι

$$|\Lambda : \Lambda_0| \geqslant |Q \cap \Lambda|.$$

Για την αντίστροφη ανισότητα, δείχνουμε ότι αν $x \in \Lambda$ τότε υπάρχει $y \in Q \cap \Lambda$ ώστε $x \in y + \Lambda_0$. Πράγματι, από την Πρόταση 7.1.7, υπάρχουν $y \in Q$ και $z \in \Lambda_0$ ώστε $x = y + z$. Αφού $x \in \Lambda$ και $z \in \Lambda_0 \subseteq \Lambda$, θα είναι $y = x - z \in \Lambda$. Άρα $y \in Q \cap \Lambda$, και $x \in y + \Lambda_0$. □

Το επόμενο θεώρημα δίνει ένα «ειδικό» ζευγάρι βάσεων για τα Λ_0 και Λ (κανονική μορφή κατά Smith):

Θεώρημα 7.1.9. *Έστω Λ_0 ένα υποπλέγμα του πλέγματος Λ στον $\mathbb{R}^n$. Υπάρχουν βάσεις $U = \{u_1, \ldots, u_n\}$ του Λ και $V = \{v_1, \ldots, v_n\}$ του Λ_0, ώστε*

$$v_i = m_i u_i, \quad 1 = i, \ldots, n$$

και

$$m_i \mid m_{i+1}, \quad i = 1, \ldots, n-1.$$

Απόδειξη. Έστω $U = \{u_i\}_{i=1}^n$ και $V = \{v_i\}_{i=1}^n$ δύο βάσεις των Λ και Λ_0 αντίστοιχα. Κάθε $v_i \in V$ γράφεται μονοσήμαντα στη μορφή

$$v_i = m_{i1}u_1 + \cdots + m_{in}u_n, \quad m_{ij} \in \mathbb{Z}.$$

Παίρνουμε έτσι έναν ακέραιο πίνακα $M = M(U, V)$ ο οποίος εξαρτάται από την επιλογή των βάσεων U και V, για τον οποίο ισχύει η σχέση πινάκων

$$V = UM^T.$$

Θεωρούμε την κλάση $\mathcal{M} = \{M(U,V),\ U$ βάση του $\Lambda,\ V$ βάση του $\Lambda_0\}$. Η κλάση $\mathcal{M}$ μένει αναλλοίωτη ως προς τη δράση των ακόλουθων μετασχηματισμών πινάκων:

(α) Αν μεταθέσουμε την i με την j γραμμή του πίνακα M, παίρνουμε τον πίνακα $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις U και $V_1 = V$ (με μετάθεση των v_i, v_j).

(β) Αν μεταθέσουμε την i με την j στήλη του πίνακα M, παίρνουμε τον πίνακα $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις $U_1 = U$ (με μετάθεση των u_i, u_j) και V.

(γ) Αν πολλαπλασιάσουμε την i γραμμή με -1, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις U και $V_1 = \{v_1, \ldots, -v_i, \ldots, v_n\}$.

(δ) Αν πολλαπλασιάσουμε την i στήλη με -1, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις $U_1 = \{u_1, \ldots, -u_i, \ldots, u_n\}$ και V.

(ε) Αν προσθέσουμε στην i-γραμμή την j-γραμμή πολλαπλασιασμένη επί κάποιο $s \in \mathbb{Z}$, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις U και $V_1 = \{v_1, \ldots, v_i + sv_j, \ldots, v_n\}$.

(στ) Αν προσθέσουμε στην i-στήλη την j-στήλη πολλαπλασιασμένη επί κάποιο $s \in \mathbb{Z}$, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις $U_1 = \{u_1, \ldots, u_i - su_j, \ldots, u_n\}$ και V.

Οι παρατηρήσεις αυτές δείχνουν ότι υπάρχει $M \in \mathcal{M}$ με $m_{11} > 0$. Αυτό φαίνεται εύκολα γιατί, ξεκινώντας με τυχόντα $M_0 \in \mathcal{M}$ και εκτελώντας κατάλληλα κάποιους από τους μετασχηματισμούς που περιγράψαμε, μπορούμε να κάνουμε οποιοδήποτε μη μηδενικό στοιχείο του M θετικό και να το φέρουμε στην $(1,1)$ θέση.

Θεωρούμε όλους τους $M \in \mathcal{M}$ με $m_{11} > 0$, και κρατάμε έναν με ελάχιστο m_{11}. (Αυτό το βήμα καθιστά την απόδειξη μη κατασκευαστική.) Τότε, $m_{11} \mid m_{i1}, m_{1j}$ για κάθε $i, j = 1, \dots n$. Πράγματι, αν σε κάποια περίπτωση είχαμε το αντίθετο, για παράδειγμα αν το m_{21} δεν ήταν πολλαπλάσιο του m_{11}, τότε κάνοντας την διαίρεση θα είχαμε $m_{21} = m_{11}\pi + \upsilon$ για κάποιο $0 < \upsilon < m_{11}$, $\upsilon \in \mathbb{Z}$. Τότε, πολλαπλασιάζοντας την πρώτη γραμμή με π και αφαιρώντας την από τη δεύτερη, θα παίρναμε $M_1 \in \mathcal{M}$ με $m_{21} = \upsilon$. Στη συνέχεια, αντιμεταθέτοντας την δεύτερη με την πρώτη γραμμή, θα παίρναμε έναν νέο πίνακα $M_2 \in \mathcal{M}$ ο οποίος στη θέση $(1,1)$ θα είχε το $\upsilon < m_{11}$, κάτι που είναι άτοπο από την επιλογή του πίνακα M.

Αφού λοιπόν $m_{11} | m_{i1}, m_{1j}$ για κάθε $i, j = 1, \dots, n$, μπορούμε, αφαιρώντας κατάλληλα πολλαπλάσια του m_{11} από κάθε γραμμή και στήλη του πίνακα, να μηδενίσουμε την πρώτη γραμμή και την πρώτη στήλη του πίνακα: να πάρουμε δηλαδή $M_1 \in \mathcal{M}$ με το m_{11} στην $(1,1)$-θέση και $m_{1j} = m_{i1} = 0$, $i, j = 2, \dots, n$. Επιπλέον μπορούμε να αποδείξουμε ότι στον M_1 το m_{11} είναι διαιρέτης όλων των m_{ij} (αλλιώς, με επιτρεπτούς μετασχηματισμούς μπορούμε να βρούμε $A \in \mathcal{M}$ ώστε $0 < a_{11} < m_{11}$).

Θεωρούμε όλους τους πίνακες $M \in \mathcal{M}$ που έχουν τις παραπάνω ιδιότητες: το $m_{11} > 0$ είναι το ελάχιστο δυνατό στην $\mathcal{M}$, τα $m_{i1}, m_{1j} = 0$ αν $i, j \neq 1$, και κάθε m_{ij} είναι πολλαπλάσιο του m_{11}. Παίρνουμε πίνακα αυτής της μορφής με το $m_{22} > 0$ και ελάχιστο, και συνεχίζουμε όπως πρίν (αγνοώντας την πρώτη γραμμή και την πρώτη στήλη, οι οποίες έχουν οριστικοποιηθεί). Σε n βήματα, θα φτάσουμε στη ζητούμενη μορφή. □

Η χρησιμότητα της κανονικής μορφής Smith φαίνεται από το επόμενο θεώρημα.

Θεώρημα 7.1.10. *Έστω Λ_0 ένα υποπλέγμα του πλέγματος Λ στον $\mathbb{R}^n$. Αν U και V είναι βάσεις των Λ και Λ_0 αντίστοιχα, και Q είναι το θεμελιώδες παραλληλεπίπεδο του Λ_0 ως προς την V, τότε*

$$|Q \cap \Lambda| = |\Lambda : \Lambda_0| = |\det M(U,V)| = \frac{\det \Lambda_0}{\det \Lambda}.$$

Απόδειξη. Η πρώτη ισότητα αποδείχθηκε στο Θεώρημα 7.1.8, και για κάθε ζευγάρι βάσεων U, V των Λ, Λ_0 έχουμε

$$|\det M(U,V)| = \frac{|\det V|}{|\det U|} = \frac{\det \Lambda_0}{\det \Lambda}.$$

Αρκεί λοιπόν να δείξουμε ότι $|\det M(U,V)| = |P \cap \Lambda|$ για *κάποιο* ζευγάρι βάσεων U, V των Λ, Λ_0. Από το Θεώρημα 7.1.9, μπορούμε να επιλέξουμε βάσεις U, V ώστε

$$v_i = m_i u_i, \quad m_i \in \mathbb{Z}, \ \ i = 1, \dots, n.$$

Τότε, είναι φανερό ότι

$$\det M(U,V) = m_1 m_2 \dots m_n.$$

Απομένει να μετρήσουμε το πλήθος των σημείων του Λ που ανήκουν στο Q. Όμως, λόγω της σχέσης $v_i = m_i u_i$ έχουμε ότι, για κάθε $i = 1, \dots, n$, στο ευθύγραμμο τμήμα $[0, v_i)$ υπάρχουν m_i

το πλήθος σημεία του Λ. Άρα στο Q θα έχουμε $m_1 m_2 \cdots m_n$ σημεία του Λ, τα $t_1 v_1 + \cdots + t_n v_n$, $t_i \in \{0, 1, \ldots, m_i - 1\}$. Αυτό αποδεικνύει το ζητούμενο. □

Παρατήρηση 7.1.11. Το Θεώρημα 7.1.10 έχει τις εξής άμεσες, αλλά ενδιαφέρουσες, συνέπειες:

(α) Αν το Λ_0 είναι υποπλέγμα του Λ,τότε για κάθε βάση V του Λ_0, το πλήθος των σημείων του Λ που ανήκουν στο θεμελιώδες παραλληλεπίπεδο του Λ_0 ως προς την V είναι σταθερό, και ίσο με $|\Lambda : \Lambda_0|$.

(β) Μία ενδιαφέρουσα ειδική περίπτωση έχουμε αν πάρουμε σαν Λ το $\mathbb{Z}^n$. Αν $v_1, \ldots, v_n$ είναι γραμμικά ανεξάρτητα διανύσματα του $\mathbb{R}^n$ με ακέραιες συντεταγμένες, τότε το παραλληλεπίπεδο Q που ορίζουν περιέχει τόσα ακέραια σημεία όσος είναι ο όγκος του. Γιατί, αν Λ_0 είναι το υποπλέγμα του $\mathbb{Z}^n$ που παράγουν τα v_i, από το Θεώρημα 7.1.10 έχουμε

$$|Q| = |\det \Lambda_0| = |\mathbb{Z}^n : \Lambda_0| = |\mathbb{Z}^n \cap Q|.$$

7.1.3 Δυϊκό πλέγμα

Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$. Το σύνολο

$$\Lambda^* := \{y \in \mathbb{R}^n : \forall x \in \Lambda, \ \langle x, y\rangle \in \mathbb{Z}\}$$

ονομάζεται *δυϊκό πλέγμα* του Λ.

Στην επόμενη πρόταση αποδεικνύουμε ότι το Λ^* είναι όντως πλέγμα, και περιγράφουμε το Λ^* συναρτήσει του Λ.

Πρόταση 7.1.12. *Το Λ^* είναι πλέγμα στον $\mathbb{R}^n$. Αν $u_1, \ldots, u_n$ είναι μια βάση του Λ, τότε τα διανύσματα $u_1^*, \ldots, u_n^*$ που ορίζονται από τις*

$$\langle u_i, u_j^*\rangle = \delta_{ij}, \quad i, j = 1, \ldots, n$$

αποτελούν βάση του Λ^*.

Απόδειξη. Παρατηρούμε ότι

$$(\mathbb{Z}^n)^* = \mathbb{Z}^n.$$

Πράγματι, αν $x = (x_1, \ldots, x_n) \in (\mathbb{Z}^n)^*$, τότε $x_i = \langle x, e_i\rangle \in \mathbb{Z}$ για κάθε $i = 1, \ldots, n$, άρα $x \in \mathbb{Z}^n$. Αντιστρόφως, αν $x \in \mathbb{Z}^n$ τότε, προφανώς $\langle x, y\rangle \in \mathbb{Z}$ για κάθε $y \in \mathbb{Z}^n$, δηλαδή $x \in (\mathbb{Z}^n)^*$.

(α) Δείχνουμε πρώτα ότι το Λ^* είναι πλέγμα. Υπάρχει $T \in GL(n)$ ώστε $\Lambda = T(\mathbb{Z}^n)$. Τότε,

$$\begin{aligned} x \in \Lambda^* &\iff \forall y \in \Lambda \ \ \langle x, y\rangle \in \mathbb{Z} \\ &\iff \forall z \in \mathbb{Z}^n \ \ \langle x, Tz\rangle \in \mathbb{Z} \\ &\iff \forall z \in \mathbb{Z}^n \ \ \langle T^* x, z\rangle \in \mathbb{Z} \\ &\iff T^* x \in (\mathbb{Z}^n)^* = \mathbb{Z}^n \\ &\iff x \in T^{-*}(\mathbb{Z}^n). \end{aligned}$$

Όμως, $T^{-*} \in GL(n)$. Άρα, το $\Lambda^* = T^{-*}(\mathbb{Z}^n)$ είναι πλέγμα.

(β) Για τον δεύτερο ισχυρισμό, ας υποθέσουμε ότι $\{u_1, \dots, u_n\}$ είναι μια βάση του Λ. Θεωρούμε τον $T \in GL(n)$ που ορίζεται από τις $T(e_i) = u_i$, $i = 1, \dots, n$. Τότε, $\Lambda = T(\mathbb{Z}^n)$. Αν θέσουμε $u_j^* = T^{-*}(e_j)$, τότε το $\{u_1^*, \dots, u_n^*\}$ είναι βάση του $T^{-*}(\mathbb{Z}^n) = \Lambda^*$, και

$$\langle u_i, u_j^* \rangle = \langle Te_i, T^{-*}e_j \rangle = \langle T^{-1}Te_i, e_j \rangle = \langle e_i, e_j \rangle = \delta_{ij}.$$

Αυτό ολοκληρώνει την απόδειξη. □

Η βάση $\{u_1^*, \dots, u_n^*\}$ του Λ^* που ορίσαμε στην Πρόταση 7.1.12 ονομάζεται *δυϊκή βάση* της $\{u_1, \dots, u_n\}$.

7.1.4 Λ-υπόχωροι

Ορισμός 7.1.13. (α) Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$. Ένας k-διάστατος γραμμικός υπόχωρος F του $\mathbb{R}^n$ ονομάζεται *Λ-υπόχωρος* αν το $F \cap \Lambda$ είναι πλέγμα στον F. Δηλαδή, αν υπάρχουν $v_1, \dots, v_k \in F$ ώστε

$$F \cap \Lambda = \{m_1 v_1 + \cdots + m_k v_k : m_i \in \mathbb{Z}\}.$$

(β) Έστω F ένας k-διάστατος Λ-υπόχωρος του $\mathbb{R}^n$. Ένα σύνολο σημείων $v_1, \dots, v_k \in \Lambda$ ονομάζεται *πρωταρχικό* για το $F \cap \Lambda$ αν τα $v_1, \dots, v_k$ αποτελούν βάση του πλέγματος $F \cap \Lambda$.

Θεώρημα 7.1.14. *Αν ο F είναι Λ-υπόχωρος και το $\{v_1, \dots, v_k\}$ πρωταρχικό για το $F \cap \Lambda$, τότε επεκτείνεται σε βάση του Λ.*

Απόδειξη. Το Λ περιέχει n γραμμικά ανεξάρτητα διανύσματα, επομένως μπορούμε να βρούμε διανύσματα $u_{k+1}, \dots, u_n \in \Lambda$ ώστε τα $v_1, \dots, v_k, u_{k+1}, \dots, u_n$ να είναι γραμμικά ανεξάρτητα. Ξεκινώντας από αυτά τα διανύσματα, κατασκευάζουμε βάση του Λ όπως στην Πρόταση 7.1.2. Στα πρώτα k βήματα, η κατασκευή γίνεται στον F, και αφού τα $v_1, \dots, v_k$ είναι βάση του $F \cap \Lambda$ παραμένουν αμετάβλητα. □

Ορισμός 7.1.15. Έστω F ένας Λ-υπόχωρος. Ορίζουμε

$$F^\perp = \{y \in \mathbb{R}^n : \langle x, y \rangle = 0, \ \ \forall x \in F\}.$$

Θεώρημα 7.1.16. *Ο $F^\perp$ είναι Λ^*-υπόχωρος.*

Απόδειξη. Ο F είναι Λ-υπόχωρος, άρα υπάρχει βάση $\{v_1, \dots, v_k\}$ του $F \cap \Lambda$. Χρησιμοποιώντας το Θεώρημα 7.1.14 την επεκτείνουμε σε βάση $\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$ του Λ. Θεωρούμε τη δυϊκή βάση $\{u_1, \dots, u_n\}$ του Λ^*. Τότε, για κάθε $k+1 \leqslant j \leqslant n$ έχουμε

$$\langle v_i, u_j \rangle = 0, \quad i = 1, \dots, k,$$

άρα $u_j \in F^\perp$, $j = k+1, \dots, n$. Τα $u_{k+1}, \dots, u_n$ είναι γραμμικά ανεξάρτητα και ανήκουν στον $F^\perp \cap \Lambda^*$, επομένως ο $F^\perp$ είναι Λ^*-υπόχωρος. □

7.2 Πρώτο θεώρημα του Minkowski

Κυρτό σώμα στον $\mathbb{R}^n$ είναι ένα μη κενό, κυρτό και συμπαγές υποσύνολο K του $\mathbb{R}^n$, που έχει μη κενό εσωτερικό. Θα λέμε ότι το κυρτό σώμα K είναι *συμμετρικό* (με κέντρο συμμετρίας το 0) αν για κάθε $x \in K$ έχουμε $-x \in K$. Πολλές φορές, θα χρειαστεί να μιλήσουμε για *ανοικτά κυρτά σώματα*. Αυτά είναι τα εσωτερικά των κυρτών σωμάτων. Ισχύει ότι: αν K είναι ένα κυρτό σώμα, τότε το K συμπίπτει με την κλειστή θήκη του εσωτερικού του.

Το *άθροισμα Minkowski* δύο μη κενών υποσυνόλων A και B του $\mathbb{R}^n$ είναι το σύνολο

$$A + B := \{a + b : a \in A, b \in B\}.$$

Εύκολα ελέγχουμε ότι αν τα A και B είναι συμπαγή (αντίστοιχα, κυρτά), τότε και το άθροισμά τους $A + B$ είναι συμπαγές (αντίστοιχα, κυρτό). Ειδικότερα, το άθροισμα δύο κυρτών σωμάτων είναι κυρτό σώμα.

Το *πρώτο θεώρημα του Minkowski* εξασφαλίζει την ύπαρξη μη μηδενικού σημείου με ακέραιες συντεταγμένες σε κάθε ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$ που έχει όγκο μεγαλύτερο από 2^n.

Θεώρημα 7.2.1. *Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Αν $|K| > 2^n$, τότε το K περιέχει τουλάχιστον ένα $u \in \mathbb{Z}^n \setminus \{0\}$.*

Το αποτέλεσμα είναι βέλτιστο: αν θεωρήσουμε τον κύβο $Q = \{x : |x_i| < 1, i = 1, \dots, n\}$, τότε $|Q| = 2^n$, αλλά $Q \cap \mathbb{Z}^n = \{0\}$. Το θεώρημα γενικεύεται άμεσα για τυχόν πλέγμα Λ στον $\mathbb{R}^n$. Αρκεί να παρατηρήσουμε ότι $\Lambda = T(\mathbb{Z}^n)$ για κάποιον $T \in GL(n)$ με $|\det T| = \det \Lambda$ και να χρησιμοποιήσουμε το θεώρημα για το συμμετρικό κυρτό σώμα $T^{-1}(K)$:

Θεώρημα 7.2.2. *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$ και έστω K ένα ανοικτό, συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Αν $|K| > 2^n \det \Lambda$, τότε το K περιέχει τουλάχιστον ένα $u \in \Lambda \setminus \{0\}$.*

Η απόδειξη θα βασιστεί στο λήμμα του Blichfeldt:

Θεώρημα 7.2.3. *Έστω M μετρήσιμο υποσύνολο του $\mathbb{R}^n$, με $|M| > 1$. Υπάρχουν $x \neq y$ στο M ώστε $x - y \in \mathbb{Z}^n \setminus \{0\}$.*

Απόδειξη. Από την υπόθεση ότι $|M| > 1$ έπεται ότι αν το M δεν είναι φραγμένο τότε η τομή του M με μπάλα κατάλληλα μεγάλης ακτίνας θα έχει όγκο μεγαλύτερο από 1. Υποθέτουμε λοιπόν, χωρίς περιορισμό της γενικότητας, ότι το M είναι φραγμένο. Θεωρούμε το θεμελιώδες παραλληλεπίπεδο του $\mathbb{Z}^n$

$$P = \{x \in \mathbb{R}^n : 0 \leqslant x_i < 1, i = 1, \dots, n\}.$$

Το σύνολο των $u \in \mathbb{Z}^n$ για τα οποία $(u + P) \cap M \neq \emptyset$, είναι πεπερασμένο. Ας υποθέσουμε ότι είναι το $\{u^1, \dots, u^{r_0}\}$. Για κάθε $r = 1, \dots, r_0$, ορίζουμε $M_r = (u^r + P) \cap M$, και θεωρούμε τη μεταφορά $M'_r = M_r - u^r \subseteq P$. Παρατηρούμε ότι

$$\sum_{r=1}^{r_0} |M'_r| = \sum_{r=1}^{r_0} |M_r| = \sum_{r=1}^{r_0} |(u^r + P) \cap M| = \sum_{u \in \mathbb{Z}^n} |(u + P) \cap M| = |M| > 1,$$

άρα τα M'_r πρέπει να επικαλύπτονται. Υπάρχουν δηλαδή $r \neq s \in \{1, \dots, r_0\}$ και $z \in M'_r \cap M'_s$. Τότε, τα $x = z + u^r$ και $y = z + u^s$ ανήκουν στο M, και $x - y = u^r - u^s \in \mathbb{Z}^n \setminus \{0\}$. □

Παρατήρηση 7.2.4. Το ίδιο ισχύει αν υποθέσουμε ότι το M είναι φραγμένο, κλειστό, και $|M| \geqslant 1$. Γιατί αν πάρουμε μια φθίνουσα ακολουθία $\lambda_r \to 1$, έχουμε $|\lambda_r M| > 1$, άρα υπάρχουν $x_r, y_r \in \lambda_r M$ ώστε $0 \neq x_r - y_r \in \mathbb{Z}^n$. Τότε, οι (x_r), (y_r) έχουν υπακολουθίες $x_{k_r} \to x \in M$, $y_{k_r} \to y \in M$, και εύκολα ελέγχουμε ότι $x - y \in \mathbb{Z}^n \setminus \{0\}$.

Απόδειξη του θεωρήματος. Θεωρούμε το $M = K/2$. Το M είναι μετρήσιμο και, από την υπόθεσή μας, $|M| > 1$. Από το Λήμμα του Blichfeldt, υπάρχουν $x, y \in M$ ώστε $0 \neq x - y \in \mathbb{Z}^n$. Όμως, από τον ορισμό του M, υπάρχουν $w_1, w_2 \in K$ με $x = w_1/2$ και $y = w_2/2$. Το K είναι συμμετρικό ως προς το 0, άρα $-w_2 \in K$, και κυρτό, άρα

$$x - y = \frac{w_1 + (-w_2)}{2} \in K.$$

Δηλαδή, $0 \neq x - y \in K \cap \mathbb{Z}^n$. □

Έστω K κλειστό κυρτό σώμα στον $\mathbb{R}^n$, το οποίο περιέχει το 0 στο εσωτερικό του. Ο *συντελεστής ασυμμετρίας* του K ως προς το 0 είναι ο μικρότερος $\sigma = \sigma(K) > 0$ για τον οποίο

$$x \in K \Longrightarrow -x \in \sigma K.$$

Παρατηρήστε ότι, $\sigma(K) \geqslant 1$ για κάθε K, με ισότητα αν και μόνο αν το K είναι συμμετρικό ως προς το 0. Ο Mahler παρατήρησε ότι η απόδειξη του θεωρήματος του Minkowski για τη συμμετρική περίπτωση, ουσιαστικά χρησιμοποιεί το γεγονός ότι $\sigma = 1$, και απέδειξε την εξής γενίκευσή του:

Θεώρημα 7.2.5. *Έστω K κυρτό σώμα στον $\mathbb{R}^n$, που περιέχει το 0 στο εσωτερικό του. Αν $|K| > (1 + \sigma(K))^n$, τότε $K \cap (\mathbb{Z}^n \setminus \{0\}) \neq \emptyset$.*

Απόδειξη. Θεωρούμε το σώμα $K_1 = (1 + \sigma)^{-1} K$. Τότε, $|K_1| > 1$, άρα υπάρχουν $x, y \in K_1$ ώστε $y - x \in \mathbb{Z}^n \setminus \{0\}$. Τα K και K_1 είναι ομοιοθετικά, άρα έχουν τον ίδιο συντελεστή ασυμμετρίας, και αφού $x \in K_1$ συμπεραίνουμε ότι $-\sigma^{-1} x \in K_1$. Τότε, χρησιμοποιώντας την κυρτότητα του K_1, βλέπουμε ότι

$$y - x = (1 + \sigma) \left(\frac{1}{1 + \sigma} y + \frac{\sigma}{1 + \sigma} (-\sigma^{-1} x) \right) \in (1 + \sigma) K_1 = K.$$

Δηλαδή, $y - x \in K \cap (\mathbb{Z}^n \setminus \{0\})$. □

7.3 Διαδοχικά ελάχιστα συμμετρικού κυρτού σώματος

Έστω K ένα ανοικτό, συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Ο Minkowski όρισε τα *διαδοχικά ελάχιστα* του K ως εξής: Για κάθε $\lambda > 0$ θεωρούμε το σώμα λK. Το K είναι φραγμένο, αν λοιπόν το λ είναι αρκετά μικρό, τότε $\lambda K \cap \mathbb{Z}^n = \{0\}$. Από την άλλη πλευρά, το K περιέχει μια μπάλα με κέντρο το 0. Αν λοιπόν το λ είναι αρκετά μεγάλο, τότε το λK περιέχει n γραμμικά ανεξάρτητα διανύσματα του $\mathbb{Z}^n$. Επομένως, για κάθε $i = 1, \ldots, n$, υπάρχουν $\lambda > 0$ τέτοιοι ώστε το λK να περιέχει τουλάχιστον i γραμμικά ανεξάρτητα διανύσματα του $\mathbb{Z}^n$. Ορίζουμε

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^n) \geqslant i\}, \quad i = 1, \ldots, n,$$

όπου $\dim(\lambda K \cap \mathbb{Z}^n)$ είναι η διάσταση του υποχώρου που παράγεται από τα ακέραια σημεία του λK.

Λήμμα 7.3.1. *Ισχύει*

$$A_i := \{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^n) \geqslant i\} = (\lambda_i, \infty).$$

Απόδειξη. Είναι φανερό ότι αν $\lambda \in A_i$ και $\mu > \lambda$, τότε $\mu \in A_i$. Άρα, το A_i είναι διάστημα. Μένει λοιπόν να δούμε ότι $\lambda_i \notin A_i$. Αν το $\lambda_i K$ περιείχε i γραμμικά ανεξάρτητα ακέραια σημεία, τότε το ίδιο θα ίσχυε και για κάποιο λK με το λ λίγο μικρότερο από το λ_i, γιατί το K έχει υποτεθεί ανοικτό. □

Οι αριθμοί λ_i ονομάζονται *διαδοχικά ελάχιστα* του K (ως προς το πλέγμα $\mathbb{Z}^n$). Είναι φανερό ότι

$$0 < \lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_n.$$

Μπορεί να συμβεί κάποιοι από τους λ_i να είναι ίσοι. Για παράδειγμα, αν $K = \{x : |x_i| < 1\}$, τότε $\lambda_1 = \cdots = \lambda_n = 1$.

Πρόταση 7.3.2. *Έστω K ανοικτό, συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Υπάρχουν γραμμικά ανεξάρτητα διανύσματα $u_1, \ldots, u_n \in \mathbb{Z}^n$ που ικανοποιούν τα εξής:*

(i) $u_i \notin \langle u_1, \ldots, u_{i-1}\rangle$, $i = 1, \ldots, n$.

(ii) $u_i \notin \lambda_i K$, $i = 1, \ldots, n$.

(iii) $u_i \in \lambda_i \overline{K}$, $i = 1, \ldots, n$.

Απόδειξη. Ορίζουμε επαγωγικά $u_1, \ldots, u_n \in \mathbb{Z}^n$ που ικανοποιούν τα (1)-(3): Υποθέτουμε ότι έχουν οριστεί τα $u_1, \ldots, u_j$, και ότι $\lambda_j < \lambda_{j+1}$ (θέτουμε $\lambda_0 = 0$ και $u_0 = 0$). Τότε $u_1, \ldots, u_j \in \lambda_{j+1} K$, και το προηγούμενο λήμμα μας εξασφαλίζει ότι

$$\dim(\lambda_{j+1} K \cap \mathbb{Z}^n) = j.$$

Δείχνουμε πρώτα ότι το $\lambda_{j+1}\overline{K}$ περιέχει τουλάχιστον $j+1$ γραμμικά ανεξάρτητα ακέραια σημεία: Θεωρούμε $\lambda' > \lambda_{j+1}$. Το $\lambda' K$ περιέχει πεπερασμένα το πλήθος ακέραια σημεία. Έστω B' το σύνολο των ακεραίων σημείων του $\lambda' K$ που δεν ανήκουν στο $\lambda_{j+1}\overline{K}$. Το B' είναι μη κενό, γιατί $\lambda' > \lambda_{j+1}$. Όλα τα $u \in B'$ έχουν θετική απόσταση από το $\lambda_{j+1}\overline{K}$, και είναι πεπερασμένα το πλήθος, άρα μπορούμε να βρούμε $\lambda \in (\lambda_{j+1}, \lambda')$ με την ιδιότητα $\lambda K \cap \mathbb{Z}^n = \lambda_{j+1}\overline{K} \cap \mathbb{Z}^n$. Όμως $\lambda > \lambda_{j+1}$, άρα $\dim(\lambda K \cap \mathbb{Z}^n) \geqslant j+1$. Έπεται ότι

$$\dim(\lambda_{j+1}\overline{K} \cap \mathbb{Z}^n) = k > j.$$

Υπάρχουν λοιπόν γραμμικά ανεξάρτητα $u_{j+1}, \ldots, u_k$ στο σύνορο του $\lambda_{j+1} K$, τα οποία δεν ανήκουν στον υπόχωρο $\langle \lambda_{j+1} K \cap \mathbb{Z}^n\rangle$. Τα $u_1, \ldots, u_k$ ικανοποιούν τα (1)-(3), και από την κατασκευή,

$$\lambda_{j+1} = \cdots = \lambda_k.$$

Συνεχίζουμε με τον ίδιο τρόπο, ορίζοντας τα u_i κατά ομάδες. □

Παρατήρηση 7.3.3. Τα λ_i ορίζονται μονοσήμαντα από το K, ενώ το $\{u_1, \ldots, u_n\}$ μπορεί να μην επιλέγεται κατά μοναδικό τρόπο. Τα διανύσματα u_i της προηγούμενης πρότασης ονομάζονται *ελαχιστικά διανύσματα* του K (ως προς το πλέγμα $\mathbb{Z}^n$).

7.4 Δεύτερο θεώρημα του Minkowski

Σύμφωνα με το πρώτο θεώρημα του Minkowski, αφού $\lambda_1 K \cap \mathbb{Z}^n = \{0\}$, το $\lambda_1 K$ πρέπει να έχει όγκο το πολύ ίσο με 2^n. Με άλλα λόγια,

$$\lambda_1^n |K| \leqslant 2^n.$$

Παίρνοντας υπ' όψιν του όλα τα διαδοχικά ελάχιστα $\lambda_1, \dots, \lambda_n$ του K, ο Minkowski απέδειξε κάτι ισχυρότερο:

Θεώρημα 7.4.1 (δεύτερο θεώρημα του Minkowski)**.** *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε,*

$$\lambda_1 \lambda_2 \cdots \lambda_n |K| \leqslant 2^n.$$

Άμεση γενίκευση του θεωρήματος για τυχόν πλέγμα Λ στον $\mathbb{R}^n$ είναι το εξής:

Θεώρημα 7.4.2. *Έστω Λ πλέγμα στον $\mathbb{R}^n$, και K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε,*

$$\lambda_1 \lambda_2 \cdots \lambda_n |K| \leqslant 2^n \det \Lambda,$$

όπου

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda K \cap \Lambda) \geqslant i\}, \quad i = 1, \dots, n.$$

Η ιδέα της απόδειξης που έδωσε ο Minkowski θα γίνει πιο καθαρή από την εξής (λανθασμένη) απόπειρα: Δίνεται το ανοικτό συμμετρικό κυρτό σώμα K στον $\mathbb{R}^n$, υποθέτουμε ότι $u_1, \dots, u_n$ είναι μια επιλογή ελαχιστικών διανυσμάτων του, και ότι

$$\lambda_1 \lambda_2 \cdots \lambda_n |K| > 2^n.$$

Θεωρούμε τον γραμμικό μετασχηματισμό T που ορίζεται από τις $T(u_i) = \lambda_i u_i$, $i = 1, \dots, n$. Τότε, το $W = T(K)$ έχει όγκο $|W| = \lambda_1 \cdots \lambda_n |K| > 2^n$, οπότε το πρώτο θεώρημα του Minkowski μας δίνει $a_1, \dots, a_n \in \mathbb{R}$ ώστε

$$0 \neq w = a_1 \lambda_1 u_1 + \cdots + a_n \lambda_n u_n \in W \cap \mathbb{Z}^n.$$

Αφού $w \neq 0$, υπάρχει $k \leqslant n$ με την ιδιότητα

$$a_k \neq 0, \quad a_{k+1} = \cdots = a_n = 0.$$

Γράφουμε το w στην εξής μορφή:

$$w = \lambda_1(a_1 u_1 + \cdots + a_k u_k) + (\lambda_2 - \lambda_1)(a_2 u_2 + \cdots + a_k u_k) + \cdots + (\lambda_k - \lambda_{k-1}) a_k u_k. \tag{7.4.1}$$

Αφού $w = T(a_1 u_1 + \cdots + a_k u_k)$, γνωρίζουμε ότι $a_1 u_1 + \cdots + a_k u_k \in K$. Ας υποθέσουμε πρός στιγμήν ότι τα διανύσματα $a_2 u_2 + \cdots + a_k u_k, \dots, a_k u_k$ είναι όλα μέσα στο K. Τότε, από την κυρτότητα του K και την (7.4.1) συμπεραίνουμε ότι

$$w \in \lambda_1 K + (\lambda_2 - \lambda_1) K + \cdots + (\lambda_k - \lambda_{k-1}) K = \lambda_k K.$$

Αυτό όμως είναι άτοπο. Θα είχαμε

$$w \in \lambda_k K \setminus \langle u_1, \dots, u_{k-1} \rangle,$$

δηλαδή το w θα ήταν ακέραιο σημείο του $\lambda_k K$ γραμμικά ανεξάρτητο από τα $u_1, \dots, u_{k-1}$, κάτι που αντιφάσκει προς τον ορισμό του λ_k και των u_i.

Ο Minkowski χρησιμοποίησε αυτήν ακριβώς την ιδέα του «μετασχηματισμού» του σώματος K:

Απόδειξη του Θεωρήματος. Όπως και πριν, θεωρούμε κάποια ελαχιστικά διανύσματα $u_1, \dots, u_n$ του K, και γράφουμε το τυχόν στοιχείο του K στη μορφή $a = a_1u_1 + \cdots + a_nu_n$.

Για κάθε $a = a_1u_1 + \cdots + a_nu_n \in \mathbb{R}^n$ και $k = 1, \dots, n-1$, ορίζουμε

$$L(a_{k+1}, \dots, a_n) = \Big\{ x = \sum_{i=1}^{n} x_i u_i \in \mathbb{R}^n : x_{k+1} = a_{k+1}, \dots, x_n = a_n \Big\},$$

τον συσχετισμένο υπόχωρο των σημείων που συμπίπτουν με το a στις συντεταγμένες $x_{k+1}, \dots, x_n$ (ως προς τη βάση $\{u_1, \dots, u_n\}$). Στη συνέχεια, ορίζουμε $b(a_{k+1}, \dots, a_n)$ το κέντρο βάρους του $K \cap L(a_{k+1}, \dots, a_n)$. [Προφανώς, $b(a_1, \dots, a_n) = a$.] Δηλαδή, η i-οστή συντεταγμένη ($i \leqslant k$) του $b(a_{k+1}, \dots, a_n)$ δίνεται από το

$$\int_{K \cap L(a_{k+1}, \dots, a_n)} x_i \, dx_k \cdots dx_1.$$

Το $b(a_{k+1}, \dots, a_n)$ ανήκει στο $K \cap L(a_{k+1}, \dots, a_n)$, και όλες οι απεικονίσεις $a \mapsto b(a_{k+1}, \dots, a_n)$ είναι παραγωγίσιμες ως προς a_i στο K.

Λήμμα 7.4.3. *Ο μετασχηματισμός $T : K \to K$ που ορίζεται από την*

$$a = (a_1, \dots, a_n) \mapsto \lambda_1 b(a_1, \dots, a_n) + (\lambda_2 - \lambda_1) b(a_2, \dots, a_n) + \cdots + (\lambda_n - \lambda_{n-1}) b(a_n)$$

είναι ένα προς ένα.

Απόδειξη. Το $b(a_{k+1}, \dots, a_n)$ γράφεται στη μορφή

$$b(a_{k+1}, \dots, a_n) = \sum_{j=1}^{k} c_j(a_{k+1}, \dots, a_n) u_j + \sum_{j=k+1}^{n} a_j u_j,$$

όπου c_j είναι συναρτήσεις που εξαρτώνται μόνο από τα $a_{k+1}, \dots, a_n$, $j = 1, \dots, k$.

Έστω $a = \sum_{k=1}^{n} a_k u_k \in K$. Τότε, $T(a) = \sum_{k=1}^{n} s_k u_k$, όπου

$$s_k = \lambda_k a_k + \sum_{j=k}^{n-1} (\lambda_{j+1} - \lambda_j) c_j(a_{k+1}, \dots, a_n) = \lambda_k a_k + h(a_{k+1}, \dots, a_n). \tag{7.4.2}$$

Για να δείξουμε ότι ο T είναι ένα προς ένα, αρκεί να ελέγξουμε ότι οι συντεταγμένες s_k προσδιορίζουν μονοσήμαντα τις συντεταγμένες a_k. Για $k = n$, η (7.4.2) δίνει $s_n = \lambda_n a_n$, άρα $a_n = s_n/\lambda_n$. Τότε,

$$s_{n-1} = \lambda_{n-1} a_{n-1} + h(s_n/\lambda_n),$$

απ' όπου προσδιορίζεται το a_{n-1}, και πηγαίνοντας προς τα πίσω προσδιορίζουμε μονοσήμαντα τα $a_{n-2}, \dots, a_1$ για τα οποία $T(a) = \sum_{k=1}^{n} s_k u_k$. □

Λήμμα 7.4.4. *Ο μετασχηματισμός T «πολλαπλασιάζει» τον όγκο του K με τον παράγοντα $\lambda_1 \cdots \lambda_n$:*

$$|T(K)| = \lambda_1 \cdots \lambda_n |K|.$$

Απόδειξη. Αφού ο T είναι ένα προς ένα και διαφορίσιμος, αρκεί να παρατηρήσουμε ότι η ορίζουσα της Ιακωβιανής του T είναι σταθερή και ίση με $\lambda_1 \cdots \lambda_n$ στο K. Αυτό είναι συνέπεια του ορισμού του T. Η Ιακωβιανή του T είναι άνω τριγωνικός πίνακας (το s_k εξαρτάται μόνο από τα $a_k, \ldots, a_n$), και

$$\frac{\partial s_k(a_k, \ldots, a_n)}{\partial a_k} = \lambda_k, \quad k = 1, \ldots, n,$$

από την (7.4.2). □

Ας υποθέσουμε τώρα ότι $\lambda_1 \cdots \lambda_n |K| > 2^n$. Από το Λήμμα 7.4.4 και το θεώρημα αντίστροφης απεικόνισης, το $T(K)$ είναι ανοικτό και φραγμένο, και $|T(K)| > 2^n$, οπότε, εφαρμόζοντας το Λήμμα του Blichfeldt για το $\frac{T(K)}{2}$, βρίσκουμε $y^1 \neq y^2 \in \frac{T(K)}{2}$ ώστε

$$\frac{y^1 - y^2}{2} \in \mathbb{Z}^n \setminus \{0\}.$$

Θεωρούμε τα (μοναδικά) $a^1 \neq a^2 \in K$ για τα οποία $T(a^1) = y^1$ και $T(a^2) = y^2$, και γράφουμε

$$a^1 = \sum_{j=1}^{n} a_j^1 u_j, \quad a^2 = \sum_{j=1}^{n} a_j^2 u_j.$$

Αφού $a^1 \neq a^2$, υπάρχει $k \leqslant n$ ώστε $a_k^1 \neq a_k^2$, και $a_j^1 = a_j^2$, $j = k+1, \ldots, n$. Τότε,

$$\begin{aligned}\frac{y^1 - y^2}{2} &= \lambda_1 \frac{1}{2}(b(a_1^1, \ldots, a_n^1) - b(a_1^2, \ldots, a_n^2)) + \cdots \\ &\quad + (\lambda_k - \lambda_{k-1}) \frac{1}{2}(b(a_k^1, \ldots, a_n^1) - b(a_k^2, \ldots, a_n^2)).\end{aligned}$$

Από την κυρτότητα και τη συμμετρία του K, και από το γεγονός ότι όλες οι b παίρνουν τιμές στο K, συμπεραίνουμε ότι

$$\frac{y^1 - y^2}{2} \in \lambda_1 K + \cdots + (\lambda_k - \lambda_{k-1})K = \lambda_k K.$$

Δηλαδή,

$$\frac{y^1 - y^2}{2} \in \lambda_k K \cap (\mathbb{Z}^n \setminus \{0\}).$$

Όμως, η k-στή συντεταγμένη του $(y^1 - y^2)/2$ (ως προς τη βάση $\{u_1, \ldots, u_n\}$) είναι

$$\frac{1}{2}\left(\lambda_k a_k^1 + h(a_{k+1}^1, \ldots, a_n^1) - \lambda_k a_k^2 - h(a_{k+1}^2, \ldots, a_n^2)\right) = \frac{1}{2}\lambda_k (a_k^1 - a_k^2) \neq 0,$$

δηλαδή το $(y^1 - y^2)/2$ είναι γραμμικά ανεξάρτητο από τα $u_1, \ldots, u_{k-1}$. Αυτό είναι άτοπο, αφού το $\lambda_k K$ δεν μπορεί να περιέχει k γραμμικά ανεξάρτητα ακέραια σημεία. □

7.5 Ελεύθερες στρέψης αβελιανές ομάδες

Λέμε ότι μια αβελιανή ομάδα G είναι ελεύθερη στρέψης αν κάθε μη μηδενικό στοιχείο της G έχει άπειρη τάξη, δηλαδή για κάθε $g \neq 0$ στην G και κάθε $m \in \mathbb{Z} \setminus \{0\}$ ισχύει $mg \neq 0$. Ένα σύνολο $\{g_i : i \in I\} \subseteq G$ λέγεται σύνολο γεννητόρων της G αν κάθε $g \in G$ αναπαρίσταται στη μορφή

$$g = \sum_{i \in I} m_i g_i,$$

όπου $m_i \in \mathbb{Z}$ και $m_i = 0$ για όλους εκτός από πεπερασμένους το πλήθος δείκτες $i \in I$. Λέμε ότι μια αβελιανή ομάδα G είναι πεπερασμένα παραγόμενη αν περιέχει πεπερασμένο σύνολο γεννητόρων. Λέμε ότι μια αβελιανή ομάδα είναι ελεύθερη αν περιέχει σύνολο $\{g_i : i \in I\}$ τέτοιο ώστε κάθε $g \in G$ να έχει μοναδική αναπαράσταση στη μορφή

$$g = \sum_{i \in I} m_i g_i,$$

όπου $m_i \in \mathbb{Z}$ και $m_i = 0$ για όλους εκτός από πεπερασμένους το πλήθος δείκτες $i \in I$. Σε αυτήν την περίπτωση, το σύνολο $\{g_i : i \in I\}$ λέγεται βάση της G. Κάθε ελεύθερη αβελιανή ομάδα είναι ελεύθερη στρέψης. Η ομάδα $G = \{0\}$ είναι η ελεύθερη αβελιανή ομάδα που έχει ως βάση το κενό σύνολο.

Για κάθε αβελιανή ομάδα G και $m \geqslant 2$ ορίζουμε

$$m * G = \{mg : g \in G\}.$$

Αφού η G είναι αβελιανή, το σύνολο $m * G$ είναι υποομάδα της G για κάθε $m \geqslant 2$. Συμβολίζουμε με $[G : m * G]$ τον δείκτη της $m * G$ στην G.

Λήμμα 7.5.1. *Έστω G ελεύθερη αβελιανή ομάδα. Αν $[G : m * G] = \infty$ τότε κάθε βάση της G είναι άπειρη. Αν $[G : 2 * G] < \infty$ τότε κάθε βάση της G έχει πληθάριθμο*

$$\frac{\log[G : 2 * G]}{\log 2}.$$

Απόδειξη. Έστω $\{g_i : i \in I\}$ μια βάση της G. Η απεικόνιση $\varphi : G \to \oplus_{i \in I} \mathbb{Z}/2\mathbb{Z}$ που ορίζεται από την

$$\varphi\Big(\sum_{i \in I} m_i g_i\Big) = (m_i + 2\mathbb{Z})_{i \in I}$$

είναι καλά ορισμένη και ομομορφισμός επί, με πυρήνα $2 * G$. Συνεπώς,

$$G/(2 * G) \simeq \oplus_{i \in I} \mathbb{Z}/2\mathbb{Z}.$$

Αν η ομάδα πηλίκο $G/(2 * G)$ είναι άπειρη, τότε το I πρέπει να είναι άπειρο σύνολο, άρα κάθε βάση της G είναι άπειρη. Αν η ομάδα πηλίκο $G/(2 * G)$ είναι πεπερασμένη, τότε το I είναι πεπερασμένο και

$$[G : 2 * G] = |G/(2 * G)| = \Big| \oplus_{i \in I} \mathbb{Z}/2\mathbb{Z} \Big| = 2^{|I|},$$

άρα κάθε βάση της G έχει πληθάριθμο $\log[G : 2 * G]/\log 2$. □

Έστω $G \neq \{0\}$ μια ελεύθερη αβελιανή ομάδα με πεπερασμένη βάση. Η τάξη της G είναι ο πληθάριθμος μιας βάσης της G. Από το Λήμμα 7.5.1 η τάξη μιας ελεύθερης αβελιανής ομάδας είναι καλά ορισμένη. Αν $G = \{0\}$ τότε λέμε ότι η G έχει τάξη 0. Αν G_1 είναι ελεύθερη αβελιανή ομάδα τάξης n_1 και G_2 είναι ελεύθερη αβελιανή ομάδα τάξης n_2, τότε η $G_1 \oplus G_2$ είναι ελεύθερη αβελιανή ομάδα τάξης $n_1 + n_2$.

Λήμμα 7.5.2. *Έστω $G \neq \{0\}$ ελεύθερη αβελιανή ομάδα πεπερασμένης τάξης. Τότε, η G είναι ισόμορφη με τον $\mathbb{Z}^n$ για κάποιον $n \geqslant 1$.*

Απόδειξη. Έστω $\{g_1, \ldots, g_n\}$ μια βάση της G. Η απεικόνιση $\varphi : G \to \mathbb{Z}^n$ που ορίζεται από την

$$\varphi\Big(\sum_{i=1}^{n} m_i g_i\Big) = (m_1, \ldots, m_n)$$

είναι καλά ορισμένη και εύκολα ελέγχουμε ότι είναι ισομορφισμός. □

Λήμμα 7.5.3. *Έστω G μια αβελιανή ομάδα, και έστω A μια ελεύθερη αβελιανή ομάδα. Έστω $\varphi : G \to A$ ομομορφισμός επί. Τότε $G = K \oplus H$, όπου K είναι ο πυρήνας της φ και H είναι μια υποομάδα της G τέτοια ώστε η $\varphi : H \to A$ να είναι ισομορφισμός.*

Απόδειξη. Έστω $\{a_i : i \in I\}$ μια βάση για την ελεύθερη αβελιανή ομάδα A. Αφού η απεικόνιση φ είναι επί, μπορούμε να βρούμε $h_i \in G$ τέτοια ώστε $\varphi(h_i) = a_i$. Έστω H η υποομάδα της G που παράγεται από το $\{h_i : i \in I\}$. Ο περιορισμός του ομομορφισμού φ στην H απεικονίζει την H επί του A. Έπεται ότι για κάθε $g \in G$ υπάρχει $h \in H$ τέτοιο ώστε $\varphi(g) = \varphi(h)$, άρα $g - h \in K$. Αυτό αποδεικνύει ότι $G = K + H$.

Έστω $h = \sum_{i \in I} m_i h_i \in H$. Τότε

$$\varphi(h) = \sum_{i \in I} m_i \varphi(h_i) = \sum_{i \in I} m_i a_i = 0$$

αν και μόνο αν $m_i = 0$ για κάθε $i \in I$, ή ισοδύναμα, $\varphi(h) = 0$ αν και μόνο αν $h = 0$. Άρα, η $\varphi : H \to A$ είναι ισομορφισμός. Έστω $g \in K \cap H$. Αφού $g \in K$ έχουμε $\varphi(g) = 0$ και αφού $g \in H$ συμπεραίνουμε ότι $g = 0$. Άρα, $K \cap H = \{0\}$ και αυτό αποδεικνύει ότι $G = K \oplus H$. □

Λήμμα 7.5.4. *Κάθε υποομάδα μιας ελεύθερης αβελιανής ομάδας τάξης n είναι ελεύθερη αβελιανή ομάδα τάξης το πολύ ίσης με n.*

Απόδειξη. Έστω G ελεύθερη αβελιανή ομάδα τάξης n, και έστω $\{g_1, \ldots, g_n\}$ μια βάση για την G. Έστω G' υποομάδα της G. Αν $G' = \{0\}$ τότε η G' έχει τάξη 0. Συνεπώς, μπορούμε να υποθέσουμε ότι $G' \neq \{0\}$.

Η απόδειξη θα γίνει με επαγωγή ως προς n. Αν $n = 1$ τότε $G = \mathbb{Z}g_1$ για κάποιο $g_1 \in G$. Έστω

$$H = \{r \in \mathbb{Z} : rg_1 \in G'\}.$$

Τότε η H είναι υποομάδα του $\mathbb{Z}$ και $H \neq \{0\}$, άρα $H = d\mathbb{Z}$ για κάποιον $d \in \mathbb{Z}$, $d \geqslant 1$. Έπεται ότι η $G' = \mathbb{Z}dg_1$ είναι ελεύθερη αβελιανή ομάδα τάξης 1.

Έστω $n \geqslant 2$ και ας υποθέσουμε ότι το λήμμα ισχύει για κάθε ελεύθερη αβελιανή ομάδα τάξης το πολύ ίσης με $n - 1$. Έστω G μια ελεύθερη αβελιανή ομάδα με βάση $\{g_1, \ldots, g_n\}$ και έστω K

η υποομάδα της G που έχει βάση το $\{g_1, \ldots, g_{n-1}\}$. Τότε, η K είναι ελεύθερη αβελιανή ομάδα τάξης $n-1$. Αν $G' \subseteq K$ τότε από την επαγωγική υπόθεση συμπεραίνουμε ότι η G' είναι ελεύθερη αβελιανή ομάδα τάξης το πολύ ίσης με $n-1$.

Ας υποθέσουμε ότι $G' \not\subseteq K$. Ο ομομορφισμός $\varphi : G \to \mathbb{Z}g_n$ που ορίζεται από την

$$\varphi\Big(\sum_{i=1}^{n} m_i g_i\Big) = m_n g_n$$

έχει πυρήνα K. Έστω $\psi : G' \to \mathbb{Z}g_n$ ο περιορισμός του ομομορφισμού φ στην G'. Από την συνθήκη $G' \not\subseteq K$ βλέπουμε ότι $\psi(G') = \mathbb{Z}dg_n$ για κάποιον $d \in \mathbb{Z}$, $d \geqslant 1$. Έστω K' ο πυρήνας του ψ. Αφού

$$K' = K \cap G' \subseteq K$$

και η K είναι ελεύθερη και έχει τάξη $n-1$, από την επαγωγική υπόθεση έπεται ότι η K' είναι ελεύθερη αβελιανή ομάδα τάξης το πολύ ίσης με $n-1$. Η ψ απεικονίζει την G' επί της ελεύθερης αβελιανής ομάδας $\mathbb{Z}dg_n$. Από το Λήμμα 7.5.3,

$$G' \simeq H' \oplus K',$$

όπου H' είναι μια υποομάδα της G' με την ιδιότητα ότι ο περιορισμός της ψ στην H' είναι ισομορφισμός. Αυτό σημαίνει ότι η H' είναι ελεύθερη αβελιανή ομάδα τάξης 1, άρα η G' είναι ελεύθερη αβελιανή ομάδα τάξης το πολύ ίσης με $(n-1)+1 = n$. □

Θεώρημα 7.5.5. *Έστω $G \neq \{0\}$ μια πεπερασμένα παραγόμενη, ελεύθερη στρέψης αβελιανή ομάδα. Τότε, η G είναι ελεύθερη αβελιανή ομάδα πεπερασμένης τάξης, άρα η G είναι ισόμορφη με το πλέγμα $\mathbb{Z}^n$ για κάποιον $n \geqslant 1$.*

Απόδειξη. Έστω $\Gamma = \{g_1, \ldots, g_k\}$ ένα πεπερασμένο σύνολο γεννητόρων της G, και έστω $\Gamma' = \{g'_1, \ldots, g'_r\}$ ένα μεγιστικό υποσύνολο του Γ με την ιδιότητα ότι $\sum_{i=1}^{r} m_i g'_i = 0$ για κάποιους $m_i \in \mathbb{Z}$ αν και μόνο αν $m_i = 0$ για κάθε $i = 1, \ldots, r$. Έστω G' η υποομάδα της G που παράγεται από το Γ'. Τότε, η G' είναι ελεύθερη αβελιανή ομάδα τάξης r. Έστω $g_i \in \Gamma$. Αφού το Γ' είναι μεγιστικό, υπάρχουν ακέραιοι $u_i, m_{i,1}, \ldots, m_{i,r}$, όχι όλοι ίσοι με μηδέν, ώστε

$$u_i g_i + m_{i,1} g'_1 + \cdots + m_{i,r} g'_r = 0.$$

Αν $u_i = 0$ τότε $m_{i,j} = 0$ για κάθε $j = 1, \ldots, r$, το οποίο είναι άτοπο. Άρα $u_i \neq 0$, και έπεται ότι $u_i g_i \in G'$. Έστω m το ελάχιστο κοινό πολλαπλάσιο των ακεραίων $|u_1|, |u_2|, \ldots, |u_k|$. Τότε $mg_i \in G'$ για κάθε $g_i \in \Gamma$. Αφού το Γ παράγει την G, έπεται ότι

$$m * G = \{mg : g \in G\} \subseteq G'.$$

Αφού η G' είναι ελεύθερη αβελιανή ομάδα πεπερασμένης τάξης, από το Λήμμα 7.5.4 έπεται ότι η υποομάδα $m*G$ είναι επίσης ελεύθερη αβελιανή ομάδα πεπερασμένης τάξης. Αφού η G είναι ελεύθερη στρέψης, η απεικόνιση $\varphi : G \to m * G$ που ορίζεται από την $\varphi(g) = mg$ είναι ισομορφισμός, άρα η G είναι ελεύθερη αβελιανή ομάδα πεπερασμένης τάξης. Τώρα το θεώρημα προκύπτει από το Λήμμα 7.5.2. □

Θεώρημα 7.5.6. *Έστω M ένα πλέγμα στον $\mathbb{R}^n$ και Λ μια υποομάδα του $\mathbb{R}^n$ τέτοια ώστε $M \subseteq \Lambda$ και $[\Lambda : M] < \infty$. Τότε, το Λ είναι πλέγμα.*

Απόδειξη. Η Λ είναι ελεύθερη στρέψης και αβελιανή διότι ο $\mathbb{R}^n$ είναι ελεύθερη στρέψης και αβελιανή ομάδα. Επίσης, $\Lambda \neq \{0\}$ διότι $M \subseteq \Lambda$. Έστω $\{b_1, \ldots, b_r\}$ μια βάση για την M. Έστω $r = [\Lambda : M]$ και $\{u_1, \ldots, u_r\}$ ένα πλήρες σύνολο αντιπροσώπων για την πεπερασμένη ομάδα πηλίκο Λ/M. Αφού κάθε στοιχείο της Λ ανήκει σε κάποια κλάση συζυγίας $u_i + M$, έπεται ότι το $\{u_1, \ldots, u_r, b_1, \ldots, b_n\}$ παράγει την ελεύθερη στρέψης ομάδα Λ. Από το Θεώρημα 7.5.5, η Λ είναι ελεύθερη αβελιανή ομάδα με πεπερασμένη τάξη m. Αφού η M είναι υποομάδα της Λ και η M είναι ελεύθερη αβελιανή ομάδα τάξης n, από το Λήμμα 7.5.4 βλέπουμε ότι $n \leqslant m$. Αφού η Λ είναι ελεύθερη, η απεικόνιση $u \mapsto ru$ είναι ισομορφισμός από την Λ στην $r * \Lambda$, άρα η $r * \Lambda$ είναι ελεύθερη αβελιανή ομάδα τάξης m. Αφού η ομάδα πηλίκο Λ/M έχει τάξη r, έπεται ότι $r(u + M) = M$, άρα $ru \in M$ για κάθε $u \in \Lambda$. Συνεπώς,

$$r * \Lambda \subseteq M.$$

Από το Λήμμα 7.5.4 έπεται ότι $m \leqslant n$. Άρα, $m = n$ και έχουμε ότι η Λ είναι ελεύθερη αβελιανή ομάδα τάξης n.

Έστω $\{a_1, \ldots, a_n\}$ ένα σύνολο γεννητόρων της Λ. Αφού η M είναι πλέγμα, περιέχει ένα σύνολο n γραμμικά ανεξάρτητων διανυσμάτων. Αφού η Λ περιέχει την M, οι γεννήτορες $a_1, \ldots, a_n$ είναι γραμμικά ανεξάρτητοι. Συνεπώς, η Λ είναι πλέγμα. □

Το επόμενο θεώρημα θα χρησιμοποιηθεί στην απόδειξη του θεωρήματος του Freiman. Έστω $m \geqslant 2$ και έστω $u = (u_1, \ldots, u_n)$ και $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$. Γράφουμε

$$u \equiv v \bmod m$$

αν $u_i \equiv v_i \bmod m$ για κάθε $i = 1, \ldots, n$.

Θεώρημα 7.5.7. *Έστω $m \geqslant 2$ και $r_1, \ldots, r_n$ ακέραιοι τέτοιοι ώστε*

$$(r_1, \ldots, r_n, m) = 1. \tag{7.5.1}$$

Θεωρούμε $r = (r_1, \ldots, r_n) \in \mathbb{Z}^n$ και ορίζουμε το σύνολο

$$\Lambda = \{u \in \mathbb{Z}^n : h \equiv qr \bmod m \ \text{ για κάποιον } q \in \mathbb{Z}\}.$$

Τότε το Λ είναι πλέγμα, και $\det(\Lambda) = m^{n-1}$. Επιπλέον, υπάρχουν θετικοί πραγματικοί αριθμοί $\lambda_1, \ldots, \lambda_n$ τέτοιοι ώστε

$$\lambda_1 \cdots \lambda_n \leqslant 4^n m^{n-1}$$

και γραμμικά ανεξάρτητα διανύσματα $b_1, \ldots, b_n \in \Lambda$, $b_j = (b_{1,j}, \ldots, b_{n,j})$, ώστε

$$|b_{i,j}| \leqslant \frac{\lambda_j}{4}$$

για κάθε $i, j = 1, \ldots, n$.

Απόδειξη. Έστω

$$M = (m * \mathbb{Z})^n = \{u \in \mathbb{Z}^n : u \equiv 0 \bmod m\}$$

το πλέγμα στον $\mathbb{R}^n$ με βάση $(me_1, \dots, me_n)$. Το M είναι υποομάδα της ομάδας Λ, και η ορίζουσα του M είναι ίση με $\det(M) = m^n$. Για κάθε ακέραιο q έχουμε

$$\{u \in \mathbb{Z}^n : u \equiv qr \bmod m\} = qr + M \in \Lambda/M.$$

Αν $q \equiv q' \bmod m$, τότε $qr + M = q'r + M$. Αν $qr + M = q'r + M$, τότε $(q - q')r \in M$, άρα $(q - q')r_i \equiv 0 \bmod m$ για κάθε $i = 1, \dots, n$. Θέτουμε $d = (q - q', m)$. Τότε,

$$\frac{q - q'}{d} r_i \equiv 0 \bmod m/d,$$

άρα

$$r_i \equiv 0 \bmod m/d$$

για κάθε $i = 1, \dots, n$. Από την (7.5.1) έπεται ότι $d = m$ και $q \equiv q' \bmod m$. Συνεπώς,

$$\Lambda = \bigcup_{q=0}^{m-1} (qr + M),$$

το οποίο δείχνει ότι $[\Lambda : M] = m < \infty$. Από το Θεώρημα 7.5.6 έπεται ότι το Λ είναι πλέγμα. Από το Θεώρημα 7.1.10 έχουμε

$$\det(\Lambda) = \frac{\det(M)}{[\Lambda : M]} = m^{n-1}.$$

Θεωρούμε το

$$K = \{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_i| < 1/4\}.$$

Το K είναι συμμετρικό κυρτό σώμα όγκου $|K| = 2^{-n}$. Από το δεύτερο θεώρημα του Minkowski, για το σώμα K και το πλέγμα Λ, βλέπουμε ότι τα διαδοχικά ελάχιστα $\lambda_1, \dots, \lambda_n$ ικανοποιούν την

$$\lambda_1 \cdots \lambda_n \leqslant \frac{2^n \det(\Lambda)}{|K|} = 4^n m^{n-1},$$

άρα υπάρχουν γραμμικά ανεξάρτητα διανύσματα $b_1, \dots, b_n \in \Lambda$ τέτοια ώστε

$$b_j = (b_{1,j}, \dots, b_{n,j}) \in \overline{\lambda_j * K} = \lambda_j * \overline{K}$$

για $j = 1, \dots, n$. Συνεπώς,

$$|b_{i,j}| \leqslant \frac{\lambda_j}{4}$$

για κάθε $i, j = 1, \dots, n$, και έχουμε το συμπέρασμα. □

ΚΕΦΑΛΑΙΟ 8

Η ανισότητα του Plünnecke

8.1 Η ανισότητα του Plünnecke

Με τον όρο *κατευθυνόμενο διμερές γράφημα* εννοούμε μια τριάδα $G = (A, B, E)$, όπου A και B είναι πεπερασμένα σύνολα (όχι κατ' ανάγκην ξένα) και $E \subseteq A \times B$ είναι ένα σύνολο διατεταγμένων ζευγών $(a, b) \in A \times B$. Γράφουμε $G : A \to B$ για να τονίσουμε το γεγονός ότι τα ζεύγη είναι διατεταγμένα (το γράφημα είναι κατευθυνόμενο). Ο συμβολισμός $a \mapsto_G b$ σημαίνει ότι $(a, b) \in E$. Για κάθε $X \subseteq A$ ορίζουμε $G(X) = \{b \in B : a \mapsto_G b \text{ για κάποιο } a \in X\}$.

Ορισμός 8.1.1 (λόγος μεγέθυνσης)**.** Έστω $G = (A, B, E)$ ένα κατευθυνόμενο διμερές γράφημα. Ο *λόγος μεγέθυνσης* $\|G\|$ του G είναι η ποσότητα

$$\|G\| = \min\left\{\frac{|G(X)|}{|X|} : X \subseteq A, X \neq \emptyset\right\}. \tag{8.1.1}$$

Ισοδύναμα, $\|G\|$ είναι ο μικρότερος αριθμός για τον οποίο ισχύει $|G(X)| \geqslant \|G\|\,|X|$ για κάθε $X \subseteq A$.

Αν $G : A \to B$ και $H : B \to C$ είναι δύο κατευθυνόμενα διμερή γραφήματα και τα A, B, C είναι ξένα, η *σύνθεση* $H \circ G : A \to C$ είναι το κατευθυνόμενο διμερές γράφημα που ορίζεται ως εξής: $a \mapsto_{H\circ G} c$ αν και μόνο αν υπάρχει $b \in B$ ώστε $a \mapsto_G b$ και $b \mapsto_H c$.

Ορισμός 8.1.2 (γράφημα Plünnecke)**.** Έστω A_0, A_1, A_2 πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Δύο διατεταγμένα διμερή γραφήματα $G_1 : A_0 \to A_1$ και $G_2 : A_1 \to A_2$ *αντιμετατίθενται* αν ισχύει το εξής: αν $a, b, c \in G$ και $a \mapsto_{G_1} a + b \mapsto_{G_2} a + b + c$, τότε $a \mapsto_{G_1} a + c \mapsto_{G_2} a + b + c$. Ένας τρόπος να σκεφτόμαστε αυτή την ιδιότητα είναι ο εξής: αν δύο διαδοχικές ακμές ενός παραλληλογράμμου βρίσκονται στο $G_1 \cup G_2$ τότε το ίδιο ισχύει και για τις άλλες δύο ακμές του παραλληλογράμμου.

Γενικότερα, για κάθε $k \geqslant 2$, αν $A_0, A_1, \ldots, A_k$ είναι πεπερασμένα υποσύνολα της G λέμε ότι μια k-άδα $(G_1, \ldots, G_k)$ γραφημάτων $G_j : A_{j-1} \to A_j$ είναι *γράφημα Plünnecke τάξης* k αν για κάθε $j = 1, \ldots, k-1$ τα γραφήματα G_j, G_{j+1} αντιμετατίθενται.

Παράδειγμα 8.1.3. Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Ορίζουμε $G_{A,B} : A \to A+B$ θέτοντας $a \mapsto_{G_{A,B}} a+b$ αν και μόνο αν $a \in A$ και $b \in B$. Τότε,

$$\|G_{A,B}\| = \min\left\{\frac{|X+A|}{|X|} : X \subseteq A,\ X \neq \emptyset\right\} \leqslant \frac{|A+B|}{|A|}. \tag{8.1.2}$$

Παρατηρήστε ότι, αν A, B και C είναι υποσύνολα της G και τα $A, A+B, A+B+C$ είναι ξένα, τότε

$$G_{A+B,C} \circ G_{A,B} = G_{A,B+C}. \tag{8.1.3}$$

Η k-άδα $(G_{A,B}, G_{A+B,B}, \ldots, G_{A+(k-1)B,B})$ είναι γράφημα Plünnecke.

Θεώρημα 8.1.4 (ανισότητα Plünnecke)**.** *Έστω $(G_1, \ldots, G_k)$ ένα γράφημα Plünnecke τάξης k. Τότε, η ακολουθία των λόγων μεγέθυνσης $\|G_i \circ \cdots \circ G_1\|^{1/i}$, $i = 1, \ldots, k$, είναι φθίνουσα. Ειδικότερα,*

$$\|G_k \circ \cdots \circ G_1\| \leqslant \|G_1\|^k. \tag{8.1.4}$$

Για την απόδειξη του θεωρήματος του Plünnecke αρκεί να δείξουμε ότι: αν $1 \leqslant i < k$ τότε

$$\|G_k \circ \cdots \circ G_1\|^{1/k} \leqslant \|G_i \circ \cdots \circ G_1\|^{1/i}. \tag{8.1.5}$$

Πράγματι, σταθεροποιώντας i με $i+1 < k$, θεωρούμε το γράφημα Plünnecke $(G_1, \ldots, G_{i+1})$ τάξης $i+1$ και εφαρμόζοντας την προηγούμενη ανισότητα παίρνουμε

$$\|G_{i+1} \circ \cdots \circ G_1\|^{1/(i+1)} \leqslant \|G_i \circ \cdots \circ G_1\|^{1/i}. \tag{8.1.6}$$

Σαν πρώτο βήμα για την απόδειξη της (8.1.5) θα δείξουμε πρώτα την ακόλουθη «κανονικοποιημένη» έκδοση της ανισότητας:

Θεώρημα 8.1.5 (κανονικοποιημένη ανισότητα Plünnecke)**.** *Έστω $(G_1, \ldots, G_k)$ ένα γράφημα Plünnecke τάξης k ώστε $\|G_k \circ \cdots \circ G_1\| \geqslant 1$. Τότε,*

$$\|G_i \circ \cdots \circ G_1\| \geqslant 1, \quad 1 \leqslant i < k. \tag{8.1.7}$$

Για την απόδειξη του θεωρήματος 8.1.5 χρησιμοποιούμε το θεώρημα του Menger. Δίνουμε πρώτα κάποιους ορισμούς. Έστω G ένα κατευθυνόμενο γράφημα και έστω A, B δύο ξένα σύνολα κορυφών του. Λέμε ότι ένα σύνολο κορυφών C είναι *τομή* που διαχωρίζει τα A και B αν αφαιρώντας το C καταστρέφουμε όλα τα κατευθυνόμενα μονοπάτια που ξεκινούν από το A και καταλήγουν στο B. Έστω Γ ένα μεγιστικό σύνολο μονοπατιών που ξεκινούν από το A, καταλήγουν στο B και (ανά δύο) έχουν ξένα σύνολα κορυφών. Αν $|\Gamma| = N$, είναι φανερό ότι κάθε τομή C πρέπει να έχει πληθάριθμο τουλάχιστον ίσο με N, αφού η C θα πρέπει να περιέχει τουλάχιστον ένα σημείο από κάθε μονοπάτι του Γ. Το θεώρημα του Menger ισχυρίζεται ότι αυτό το φράγμα είναι ακριβές.

Θεώρημα 8.1.6 (Menger)**.** *Έστω G, A, B και Γ όπως παραπάνω. Υπάρχει τομή C που διαχωρίζει τα A και B και έχει πληθάριθμο $|C| = N = |\Gamma|$.*

Θεωρούμε ένα γράφημα Plünnecke που αποτελείται από τα γραφήματα $G_1 : A_0 \to A_1, \dots, G_k : A_{k-1} \to A_k$. Αντικαθιστώντας την G με την $G \times \mathbb{Z}$ και κάθε A_j με το $A \times \{j\}$, μπορούμε πάντα να υποθέτουμε ότι τα A_j είναι ξένα. Θέτουμε $G = G_1 \cup \dots \cup G_k$. Τότε, το G είναι κατευθυνόμενο γράφημα στο $A_0 \cup A_1 \cup \dots \cup A_k$. Θέτουμε $A = A_0$, $B = A_k$ και θεωρούμε ένα μεγιστικό σύνολο $\Gamma = \{\gamma_1, \dots, \gamma_N\}$ ξένων μονοπατιών από το A στο B. Παρατηρήστε ότι $|A_0| \geqslant N$, αφού όλα τα μονοπάτια γ_j ξεκινούν από το A_0 και έχουν ξένα σύνολα κορυφών.

Από το θεώρημα του Menger, υπάρχει τομή $C = \{c_1, \dots, c_N\}$ στο G που διαχωρίζει το A_0 από το A_k ώστε κάθε c_j να ανήκει στο γ_j, $j = 1, \dots, N$.

Για κάθε $i = 1, \dots, k$ ορίζουμε $C_i = C \cap A_i$. Υποθέτουμε ότι $C_i \neq \emptyset$ και γράφουμε $C_i = \{c_1, \dots, c_m\}$, όπου $1 \leqslant m \leqslant N$. Έστω Γ ένα μεγιστικό σύνολο μονοπατιών από το A_0 στο A_k. Για κάθε $j = 1, \dots, m$, το c_j είναι κορυφή για ακριβώς ένα μονοπάτι γ_j του Γ. Άρα, υπάρχουν μοναδικά $c_j^- \in A_{i-1}$ και $c_j^+ \in A_{i+1}$ ώστε οι ακμές $c_j^- \to c_j$ και $c_j \to c_j^+$ να ανήκουν στο γ_j. Θεωρούμε τα σύνολα $C_i^\pm = \{c_1^\pm, \dots, c_m^\pm\} \subseteq A_{i\pm1}$. Αφού τα μονοπάτια γ_j είναι ξένα, έχουμε $|C_i^-| = |C_i| = |C_i^+|$. Επίσης, τα C_i^-, C_i^+ είναι ξένα προς το C, αφού κάθε γ_j περιέχει ακριβώς ένα σημείο του C.

Λήμμα 8.1.7. *Το σύνολο $C' = (C \setminus C_i) \cup C_i^-$ είναι επίσης τομή στο G που διαχωρίζει τα A και B.*

Απόδειξη. Έστω ότι το C' δεν είναι τομή. Τότε, υπάρχει μονοπάτι γ από το A_0 στο A_k το οποίο δεν τέμνει το C'. Αφού το C είναι τομή, το γ τέμνει το C. Αναγκαστικά, το γ τέμνει το A_{i-1} σε μια κορυφή $v \in A_{i-1}$ που δεν ανήκει ούτε στο C_{i-1} ούτε στο C_i^-. Επιπλέον, η τομή του γ με το C ανήκει στο C_i. Γράφουμε s_i για το πλήθος των ακμών από το C_i^- στο C_i, s_2 για το πλήθος των ακμών από το $C_i^- \cup \{v\}$ στο C_i και s_3 για το πλήθος των ακμών από το C_i στο C_i^+. Για να καταλήξουμε σε άτοπο, θα δείξουμε ότι

$$s_1 < s_2, \quad s_2 \leqslant s_3, \quad s_3 \leqslant s_1.$$

Η ανισότητα $s_1 < s_2$ είναι φανερή, γιατί το v δεν ανήκει στο C_i^- και υπάρχει ακμή του γ που πηγαίνει από το v στο C_i.

Για την ανισότητα $s_3 \leqslant s_1$ θα ορίσουμε 1-1 συνάρτηση μεταξύ του συνόλου των ακμών από το C_i στο C_i^+ και του συνόλου των ακμών από το $C_i^- \cup \{v\}$ στο C_i. Θεωρούμε τυχούσα ακμή $c_j \to c_{j_1}^+$ από το C_i στο C_i^+. Αφού τα G_i και G_{i+1} αντιμετατίθενται και έχουμε $(c_j^- \to c_j) \in G_i$ και $(c_j \to c_{j_1}^+) \in G_{i+1}$, συμπεραίνουμε ότι $(c_j^- \to c') \in G_i$ και $(c' \to c_{j_1}^+) \in G_{i+1}$, όπου $c' = c_j^- + c_{j_1}^+ - c_j$. Επιπλέον, $c' \in C_i$ (αλλιώς θα μπορούσαμε να βρούμε μονοπάτι από το A_0 στο A_k το οποίο αποφεύγει την τομή C, χρησιμοποιώντας το γ_j ως το c_j^-, μετά την διαδρομή $c_j^- \to c' \to c_{j_1}^+$ και μετά χρησιμοποιώντας το γ_{j_1} ως το A_k). Έτσι, έχουμε μια ακμή $(c_j^- \to c')$ από το C_i^- στο C_i. Τώρα, μπορούμε να ελέγξουμε ότι η απεικόνιση που στέλνει την $(c_j \to c_{j_1}^+)$ στην $(c_j^- \to c')$ είναι 1-1.

Η απόδειξη της ανισότητας $s_2 \leqslant s_3$ είναι παρόμοια: όταν έχουμε μια ακμή που ξεκινάει από το v, ορίζουμε ένα μονοπάτι που αποφεύγει την C χρησιμοποιώντας το γ ως το v. □

Λήμμα 8.1.8. *Αν $\|G_k \circ \dots \circ G_1\| \geqslant 1$ τότε $|A_0| = N$.*

Απόδειξη. Έχουμε ήδη παρατηρήσει ότι $|A_0| \geqslant N$, αφού όλα τα μονοπάτια γ_j ξεκινούν από το A_0 και έχουν ξένα σύνολα κορυφών.

Για την αντίστροφη ανισότητα, εφαρμόζοντας διαδοχικά το προηγούμενο λήμμα, βρίσκουμε μια τομή $C_0 \cup C_k$ που περιέχεται στο $A_0 \cup A_k$: $C_0 \subseteq A_0$ και $C_k \subseteq A_k$. Αυτό σημαίνει ότι κάθε μονοπάτι που ξεκινάει από το $X = A_0 \setminus C_0$ καταλήγει στο C_k. Από τον ορισμό του λόγου μεγέθυνσης έχουμε

$$\|G_k \circ \cdots \circ G_1\| \leqslant \frac{|C_k|}{|X|}. \tag{8.1.8}$$

Από την άλλη πλευρά, $|C_0| + |C_k| = N$ και $|X| = |A_0| - |C_0|$. Τότε,

$$\frac{N - |C_0|}{|A_0| - |C_0|} \geqslant \|G_k \circ \cdots \circ G_1\| \geqslant 1, \tag{8.1.9}$$

άρα $N \geqslant |A_0|$. □

Απόδειξη του Θεωρήματος 8.1.5. Αφού $|A_0| = N$, κάθε κορυφή $v \in A_0$ είναι αρχική κορυφή για ακριβώς ένα μονοπάτι της Γ. Η Γ αποτελείται από ξένα μονοπάτια, συνεπώς $|(G_i \circ \cdots \circ G_1)(X)| \geqslant |X|$ για κάθε $X \subseteq A_0$. Έπεται ότι $\|G_i \circ \cdots \circ G_1\| \geqslant 1$. □

Επόμενος στόχος μας είναι να δείξουμε πώς προκύπτει το θεώρημα Plünnecke από το θεώρημα 8.1.5. Εδώ χρησιμοποιείται το τέχνασμα της «ύψωσης σε δύναμη»: χρησιμοποιώντας την κανονικοποιημένη ανισότητα του Θεωρήματος 8.1.5 αποδεικνύουμε πρώτα μια ασθενέστερη μορφή του θεωρήματος Plünnecke. Εφαρμόζοντας αυτή την ασθενέστερη ανισότητα σε μια μεγάλη δύναμη του γραφήματός μας και παίρνοντας όριο, έχουμε το ζητούμενο.

Θα χρειαστεί να ορίσουμε την έννοια του γινομένου που θα χρησιμοποιήσουμε: αν $G : A \to B$ και $G' : A' \to B'$ είναι διμερή γραφήματα, το *ευθύ άθροισμα* $G \oplus G' : A \oplus A' \to B \oplus B'$ ορίζεται ως εξής: $(a, a') \mapsto_{G \oplus G'} (b, , b')$ αν και μόνο αν $a \mapsto_G b$ και $a' \mapsto_{G'} b'$.

Λήμμα 8.1.9. *Ισχύουν οι ισότητες*

$$\|G \oplus H\| = \|G\| \, \|H\| \tag{8.1.10}$$

και

$$(G_k \circ \cdots \circ G_1) \oplus (H_k \circ \cdots \circ H_1) = (G_k \oplus H_k) \circ \cdots \circ (G_1 \oplus H_1). \tag{8.1.11}$$

Απόδειξη. Ας υποθέσουμε ότι $G : A \to B$ και $H : C \to D$. Θεωρούμε $X \subseteq A$ και $Y \subseteq C$ ώστε

$$\|G\| = \frac{|G(X)|}{|X|} \text{ και } \|H\| = \frac{|H(Y)|}{|Y|}. \tag{8.1.12}$$

Τότε, $X \times Y \subseteq A \times C$ και $(G \oplus H)(X \times Y) \subseteq G(X) \times H(Y)$. Συνεπώς,

$$\|G\| \, \|H\| = \frac{|G(X)| \, |H(Y)|}{|X| \, |Y|} \geqslant \frac{|(G \oplus H)(X \times Y)|}{|X \times Y|} \geqslant \|G \oplus H\|. \tag{8.1.13}$$

Για την αντίστροφη κατεύθυνση θεωρούμε τυχόν $U \subseteq A \times C$ και γράφουμε $U = \bigcup(\{a\} \times Y_a)$, όπου η ένωση είναι πάνω από όλα τα a για τα οποία το $Y_a = \{c \in C : (a, c) \in U\}$ είναι μη κενό. Ορίζουμε

$$Z = \{(a, d) : \text{ υπάρχει } b \in D \text{ ώστε } (a, b) \in U \text{ και } b \mapsto_H d\} \tag{8.1.14}$$

και γράφουμε $Z = \bigcup(X_d \times \{d\})$, όπου η ένωση είναι πάνω από όλα τα d για τα οποία το $X_d = \{a \in A : (a,d) \in Z\}$ είναι μη κενό.

Παρατηρούμε ότι

$$|Z| = \sum |H(Y_a)| \geqslant \|H\| \sum |Y_a| = \|H\|\,|U|. \tag{8.1.15}$$

Από την άλλη πλευρά, $(G \oplus H)(U) = \bigcup(G(X_d) \times \{d\})$, άρα

$$|(G \oplus H)(U)| = \sum |G(X_d)| \geqslant \|G\| \sum |X_d| = \|G\|\,|Z|. \tag{8.1.16}$$

Συνδυάζοντας τις δύο ανισότητες βλέπουμε ότι

$$|(G \oplus H)(U)| \geqslant \|G\|\,\|H\|\,|U|, \tag{8.1.17}$$

απ' όπου έπεται ότι $\|G \oplus H\| \geqslant \|G\|\,\|H\|$.

Ο δεύτερος ισχυρισμός προκύπτει απλά από τους ορισμούς. □

Λήμμα 8.1.10. *Έστω $k \geqslant 2$ και $(G_1, \dots, G_k)$ ένα γράφημα Plünnecke τάξης k. Τότε, για κάθε $m \geqslant 1$,*

$$\|G_k \circ \cdots \circ G_1\|^{1/k} \leqslant C_{i,k}\,\|G_i \circ \cdots \circ G_1\|^{1/i} \tag{8.1.18}$$

για κάποια σταθερά $C_{i,k}$ που εξαρτάται μόνο από τα i και k.

Απόδειξη. Υποθέτουμε πρώτα ότι $\|G_k \circ \cdots \circ G_1\|^{1/k} \leqslant 1$ και θεωρούμε τον μικρότερο φυσικό N για τον οποίο

$$\|G_k \circ \cdots \circ G_1\|^{1/k} \geqslant \frac{k}{N}. \tag{8.1.19}$$

Τότε $N \geqslant k \geqslant 2$ και από την επιλογή του N έπεται ότι

$$\|G_k \circ \cdots \circ G_1\|^{1/k} < \frac{k}{N-1} \leqslant \frac{2k}{n}. \tag{8.1.20}$$

Θεωρούμε ένα «βοηθητικό» γράφημα Plünnecke $(H_1, \dots, H_k)$ τάξης k, το οποίο ορίζεται με την ακόλουθη διαδικασία: θεωρούμε τη συνήθη βάση $E = \{e_1, \dots, e_N\}$ του $\mathbb{Z}^N$ και θέτουμε

$$(H_1, \dots, H_k) = (G_{0,E}, G_{E,E}, G_{2E,E}, \dots, G_{(k-1)E,E}) \tag{8.1.21}$$

με το συμβολισμό του Παραδείγματος 8.1.3. Με άλλα λόγια, $u \mapsto_{H_i} u + e_j$ αν το u είναι άθροισμα $i-1$ βασικών διανυσμάτων και $1 \leqslant j \leqslant n$. Ελέγχουμε εύκολα ότι το iE έχει $\frac{(N+i-1)!}{(N-1)!i!}$ στοιχεία. Αφού

$$\frac{N^i}{i^i} < \frac{N^i}{i!} \leqslant \frac{(N+i-1)!}{(N-1)!i!} \leqslant N^i, \tag{8.1.22}$$

συμπεραίνουμε ότι

$$\frac{1}{i}N \leqslant \|H_i \circ \cdots \circ H_1\|^{1/i} \leqslant N. \tag{8.1.23}$$

Θεωρούμε το γράφημα $G' = G \oplus H$. Χρησιμοποιώντας το Λήμμα 8.1.9, παίρνουμε

$$\|G'\|^{1/k} = \|G\|^{1/k}\|H\|^{1/k} \geqslant \frac{k}{N}\frac{N}{k} = 1, \tag{8.1.24}$$

δηλαδή το G' ικανοποιεί την υπόθεση του Θεωρήματος 8.1.4. Εφαρμόζοντας το θεώρημα για το G' βλέπουμε ότι, για κάθε $1 \leqslant\leqslant k$,

$$\|G'_1 \circ \cdots \circ G'_1\|^{1/i} = \|G_i \circ \cdots \circ G_1\|^{1/i}\|H_i \circ \cdots \circ H_1\|^{1/i} \geqslant 1. \tag{8.1.25}$$

Αφού $\|H_i \circ \cdots \circ H_1\|^{1/i} \leqslant N$, έπεται ότι

$$\|G_i \circ \cdots \circ G_1\|^{1/i} \geqslant \frac{1}{N} \geqslant \frac{1}{2k}\|G_k \circ \cdots \circ G_1\|^{1/k}, \tag{8.1.26}$$

το οποίο αποδεικνύει το λήμμα σε αυτή την περίπτωση.

Στην περίπτωση που $\|G_k \circ \cdots \circ G_1\|^{1/k} > 1$, ορίζουμε N να είναι ο μεγαλύτερος φυσικός για τον οποίο $\|G_k \circ \cdots \circ G_1\|^{1/k} \geqslant N$. Αντικαθιστώντας το γράφημα Plünnecke $(H_1, \ldots, H_k)$ με το ανάστροφο γράφημα $(H_k^*, \ldots, H_1^*)$ το οποίο προκύπτει αν αντιστρέψουμε τις φορές όλων των ακμών, ελέγχουμε ότι

$$\frac{1}{i}\frac{1}{N} \leqslant \|H_i^* \circ \cdots \circ H_1^*\|^{1/i} \leqslant \frac{1}{N}. \tag{8.1.27}$$

Τα υπόλοιπα βήματα της απόδειξης μένουν ως έχουν. □

Απόδειξη του Θεωρήματος 8.1.4. Εφαρμόζουμε το Θεώρημα 8.1.5 για το γράφημα $G^{\oplus m}$, $m \in \mathbb{N}$. Χρησμοποιώντας το Λήμμα 8.1.9 και το Λήμμα 8.1.10 βλέπουμε ότι

$$\|G_k \circ \cdots \circ G_1\|^{m/k} \leqslant C_{i,k}\|G_i \circ \cdots \circ G_1\|^{m/i} \tag{8.1.28}$$

για κάθε $m \in \mathbb{N}$. Παίρνοντας m-οστές ρίζες και αφήνοντας το $m \to \infty$ συμπεραίνουμε ότι $\|G_k \circ \cdots \circ G_1\|^{1/k} \leqslant \|G_i \circ \cdots \circ G_1\|^{1/i}$. □

8.2 Εφαρμογές: εκτιμήσεις για αθροίσματα συνόλων σε ομάδες

Εφαρμόζοντας το θεώρημα στην k-άδα $(G_{A,B}, G_{A+B,B}, \ldots, G_{A+(k-1)B,B})$ παίρνουμε το εξής:

Θεώρημα 8.2.1 (ανισότητα Plünnecke)**.** *Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G που ικανοποιούν την $|A+B| \leqslant c_1|A|$. Τότε, για κάθε $k \in \mathbb{N}$ υπάρχει $X \subseteq A$ ώστε*

$$|X + kB| \leqslant c_1^k|X|. \tag{8.2.1}$$

Ειδικότερα,

$$|kB| \leqslant c_1^k|A|. \tag{8.2.2}$$

Απόδειξη. Θεωρούμε το γράφημα Plünnecke $(G_{A,B}, G_{A+B,B}, \dots, G_{A+(k-1)B,B})$. Από την υπόθεση έχουμε

$$\|G_{A,B}\| \leqslant \frac{|A+B|}{|A|} \leqslant c_1. \tag{8.2.3}$$

Τότε, το Θεώρημα 8.1.4 μας εξασφαλίζει ότι

$$\|G_{A+(k-1)B,B} \circ \cdots \circ G_{A+B,B} \circ G_{A,B}\| \leqslant c_1^k. \tag{8.2.4}$$

Αυτό σημαίνει ότι υπάρχει $X \subseteq A$ ώστε

$$|(G_{A+(k-1)B,B} \circ \cdots \circ G_{A+B,B} \circ G_{A,B})(X)| \leqslant c_1^k |X|. \tag{8.2.5}$$

Όμως, $(G_{A+(k-1)B,B} \circ \cdots \circ G_{A+B,B} \circ G_{A,B})(X) = X + kB$, συνεπώς $|X+kB| \leqslant c_1^k|X|$. □

Από αυτή την ανισότητα και από την τριγωνική ανισότητα του Ruzsa έπεται το θεώρημα Plünnecke και Ruzsa:

Θεώρημα 8.2.2 (θεώρημα Plünnecke–Ruzsa)**.** *Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G ώστε $|A+B| \leqslant c_1|A|$. Τότε,*

$$|nB - mB| \leqslant c_1^{n+m}|A| \tag{8.2.6}$$

για κάθε $n, m \geqslant 1$. Ειδικότερα, αν $|A \pm A| \leqslant c_1|A|$ τότε $|nA - nA| \leqslant c_1^{2n}|A|$ για κάθε $n \geqslant 1$.

Απόδειξη. Από το Θεώρημα 8.2.1 υπάρχει $X \subseteq A$ ώστε

$$|X + nB| \leqslant c_1^n |X|.$$

Πάλι από το Θεώρημα 8.2.1, υπάρχει $Y \subseteq X$ ώστε

$$|Y + mB| \leqslant c_1^m |Y|.$$

Εφαρμόζοντας την τριγωνική ανισότητα $|U|\,|V-W| \leqslant |U+V|\,|U+W|$ για τα Y, nB και mB παίρνουμε

$$|Y|\,|nB - mB| \leqslant |Y+nB|\,|Y+mB| \leqslant |X+nB|\,|Y+mB| \leqslant c_1^n|X|\,c_1^m|Y|.$$

Έπεται ότι

$$|nB - mB| \leqslant c_1^{n+m}|X| \leqslant c_1^{n+m}|A|.$$

□

ΚΕΦΑΛΑΙΟ 9

Το θεώρημα του Freiman

9.1 Πολυδιάστατες αριθμητικές πρόοδοι

Τα απλά αντίστροφα θεωρήματα της προσθετικής θεωρίας αριθμών ισχυρίζονται ότι αν για κάποιο πεπερασμένο σύνολο A ακεραίων γνωρίζουμε ότι το $2A$ έχει μικρό πληθάριθμο, π.χ. $|2A| \leqslant 3|A|-4$, τότε μπορούμε να συμπεράνουμε ότι το A είναι μεγάλο υποσύνολο κάποιας συνήθους αριθμητικής προόδου. Το θεώρημα του Freiman γενικεύει αποτελέσματα αυτού του τύπου. Ισχυρίζεται ότι αν A είναι ένα πεπερασμένο σύνολο ακεραίων τέτοιο ώστε το $2A$ να έχει μικρό πληθάριθμο, τότε το A είναι μεγάλο υποσύνολο μιας πολυδιάστατης αριθμητικής προόδου. Η ακριβής διατύπωση αυτού του αντίστροφου θεωρήματος είναι η εξής.

Θεώρημα 9.1.1 (Freiman). *Έστω A ένα πεπερασμένο σύνολο ακεραίων τέτοιο ώστε $|2A| \leqslant c|A|$. Υπάρχουν ακέραιοι a και $q_1, \dots, q_n, \ell_1, \dots, \ell_n$ τέτοιοι ώστε*

$$A \subseteq Q = \{a + x_1q_1 + \cdots + x_nq_n : 0 \leqslant x_i < \ell_i \ \text{ για κάθε } i = 1, \dots, n\},$$

όπου $|Q| \leqslant c'|A|$ και οι n και c' εξαρτώνται μόνο από τη σταθερά c.

Σε αυτό το κεφάλαιο θα περιγράψουμε την απόδειξη ενός θεωρήματος του Ruzsa το οποίο γενικεύει το θεώρημα του Freiman.

Δίνουμε αρχικά κάποιους ορισμούς. Έστω $a, q_1, \dots, q_n$ στοιχεία μιας αβελιανής ομάδας G, και έστω $\ell_1, \dots, \ell_n$ θετικοί ακέραιοι. Το σύνολο

$$Q = Q(a; q_1, \dots, q_n; \ell_1, \dots, \ell_n) = \{a + x_1q_1 + \cdots + x_nq_n : 0 \leqslant x_i < \ell_i\}$$

ονομάζεται n-διάστατη αριθμητική πρόοδος στην G. Το μήκος της Q είναι ο $\ell(Q) = \ell_1 \cdots \ell_n$. Παρατηρήστε ότι $|Q| \leqslant \ell(Q)$. Λέμε ότι η Q είναι γνήσια αν $|Q| = \ell(Q)$.

Ένα σύνολο μπορεί να έχει περισσότερες από μία αναπαραστάσεις στη μορφή πολυδιάστατης αριθμητικής προόδου, μάλιστα αυτές οι αναπαραστάσεις μπορεί να έχουν διαφορετικές διαστάσεις και μήκη.

Θεώρημα 9.1.2. *Έστω G μια αβελιανή ομάδα και έστω Q και Q' πολυδιάστατες αριθμητικές πρόοδοι στην G διαστάσεων n και n' και μηκών ℓ και ℓ' αντίστοιχα. Τότε*

(i) *Το $Q+Q'$ είναι πολυδιάστατη αριθμητική πρόοδος διάστασης $n+n'$ και μήκους $\ell\ell'$.*

(ii) *Το $Q-Q$ είναι αριθμητική πρόοδος διάστασης n και μήκους $\ell(Q-Q)<2^n\ell$.*

(iii) *Αν η Q είναι γνήσια, τότε $\ell(hQ)<h^n|Q|$.*

(iv) *Κάθε πεπερασμένο υποσύνολο F μιας ομάδας είναι υποσύνολο μιας αριθμητικής προόδου διάστασης $|F|$ και μήκους $2^{|F|}$.*

Απόδειξη. Έστω $Q=Q(a;q_1,\dots,q_n;\ell_1,\dots,\ell_n)$ και $Q'=Q(a';q'_1,\dots,q'_{n'};\ell'_1,\dots,\ell'_{n'})$. Τότε, το σύνολο

$$\begin{aligned}Q+Q'=\{&a+a'+x_1q_1+\cdots+x_nq_n+x'_1q'_1+\cdots+x_{n'}q'_{n'}:\\&0\leqslant x_i<\ell_i,0\leqslant x'_j<\ell'_j\}\end{aligned}$$

είναι αριθμητική πρόοδος διάστασης $n+n'$ και μήκους

$$\ell(Q+Q')=\ell_1\cdots\ell_n\ell'_1\cdots\ell'_{n'}=\ell(Q)\ell(Q').$$

Όμοια,

$$Q-Q=\{y_1q_1+\cdots+y_nq_n:-\ell_i<x_i<\ell_i\}=Q(b;q_1,\dots,q_n;m_1,\dots,m_n),$$

όπου

$$b=-\sum_{i=1}^n(\ell_i-1)q_i$$

και

$$m_i=2\ell_i-1,$$

άρα το $Q-Q$ είναι αριθμητική πρόοδος διάστασης n και μήκους

$$\ell(Q-Q)=m_1\cdots m_n<2^n\ell_1\cdots\ell_n=2^n\ell(Q).$$

Παρατηρούμε ότι το hQ αναπαρίσταται στη μορφή

$$hQ=Q(ha;q_1,\dots,q_n;h(\ell_1-1)+1,\dots,h(\ell_n-1)+1),$$

άρα, αν η Q είναι γνήσια, έχουμε

$$\ell(hQ)\leqslant\prod_{i=1}^n(h(\ell_i-1)+1)<\prod_{i=1}^nh\ell_i=h^n|Q|.$$

Αν F είναι πεπερασμένο σύνολο με $|F|=n$, ας πούμε $F=\{f_1,\dots,f_n\}$, τότε

$$F\subseteq\{x_1f_1+\cdots+x_nf_n:0\leqslant x_i<2\}=Q(0;f_1,\dots,f_n;2,\dots,2)=Q,$$

όπου Q είναι n-διάστατη αριθμητική πρόοδος μήκους 2^n. □

9.2 Ισομορφισμοί Freiman

Έστω G και H αβελιανές ομάδες, και έστω $A \subseteq G$ και $B \subseteq H$. Έστω $h \geqslant 2$. Μια απεικόνιση $\varphi : A \to B$ λέγεται *ομοιομορφισμός Freiman τάξης* h αν

$$\varphi(a_1) + \cdots + \varphi(a_h) = \varphi(a'_1) + \cdots + \varphi(a'_h)$$

για κάθε $a_1, \ldots, a_h, a'_1, \ldots, a'_h \in A$ που ικανοποιούν την

$$a_1 + \cdots + a_h = a'_1 + \cdots + a'_h.$$

Τότε, η απεικόνιση $\varphi^{(h)} : hA \to hB$ με

$$\varphi^{(h)}(a_1 + \cdots + a_h) = \varphi(a_1) + \cdots + \varphi(a_h)$$

είναι καλά ορισμένη. Αν η $\varphi : A \to B$ είναι ένα προς ένα και επί, και ισχύει ότι

$$a_1 + \cdots + a_h = a'_1 + \cdots + a'_h$$

αν και μόνο αν

$$\varphi(a_1) + \cdots + \varphi(a_h) = \varphi(a'_1) + \cdots + \varphi(a'_h),$$

τότε η φ λέγεται *ισομορφισμός Freiman τάξης* h και η $\varphi^{(h)} : A \to B$ είναι επίσης ένα προς ένα και επί. Οι ισομοφισμοί Freiman τάξης 2 θα λέγονται απλώς *ισομορφισμοί Freiman*.

Αν $\varphi : A \to B$ είναι ομομορφισμόε (αντίστοιχα ισομορφισμός) Freiman τάξης h και $\psi : B \to C$ είναι ομομορφισμός (αντίστοιχα ισομορφισμός) Freiman τάξης h, τότε η $\psi \circ \varphi : A \to C$ είναι ομομορφισμός (αντίστοιχα ισομορφισμός) Freiman τάξης h.

Έστω $\varphi : A \to B$ ισομορφισμός Freiman τάξης h. Τότε η φ είναι ισομορφισμός Freiman τάξης h' για κάθε $h' \leqslant h$. Αν $A' \subseteq A$ και $B' = \varphi(A')$, τότε η απεικόνιση $\varphi : A' \to B'$ είναι επίσης ισομορφισμός Freiman τάξης h.

Αν $f : G \to H$ είναι ομομορφισμός ομάδων, τότε η f είναι ομομορφισμός Freiman τάξης h και $f^{(h)} = f$ για κάθε $h \geqslant 2$. Αν η f είναι ισομορφισμός ομάδων, τότε η f είναι ισομορφισμός Freiman τάξης h για κάθε $h \geqslant 2$.

Αν η $\varphi : G \to H$ είναι αφινική απεικόνιση, δηλαδή απεικόνιση της μορφής $\varphi(x) = a + f(x)$ όπου $a \in H$ και η $f : G \to H$ είναι ομομορφισμός (αντίστοιχα ισομορφισμός) ομάδων, τότε η φ είναι ομομορφισμός (αντίστοιχα ισομορφισμός) Freiman τάξης h και $\varphi^{(h)}(x) = ha(x)$ για κάθε $h \geqslant 2$.

Έστω $\{e_1, \ldots, e_n\}$ η συνήθης βάση του $\mathbb{R}^n$. Έστω $\ell_1, \ldots, \ell_n$ θετικοί ακέραιοι, και P το θεμελιώδες παραλληλεπίπεδο του πλέγματος που παράγεται από τα $\ell_1 e_1, \ldots, \ell_n e_n$. Το *ακέραιο παραλληλεπίπεδο* $I(P)$ ορίζεται ως εξής:

$$I(P) = P \cap \mathbb{Z}^n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : 0 \leqslant x_i < \ell_i\}.$$

Παρατηρήστε ότι $|I(P)| = \ell_1 \cdots \ell_n$. Για $h \geqslant 2$ έχουμε

$$hI(P) = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : 0 \leqslant x_i < h(\ell_i - 1) + 1\}$$

και

$$|hI(P)| = \prod_{i=1}^{n} (h(\ell_i - 1) + 1) < h^n |I(P)|.$$

Έστω $a, q_1, \dots, q_n \in \mathbb{Z}$ και έστω $Q = Q(a; q_1, \dots, q_n; \ell_1, \dots, \ell_n)$ μια n-διάστατη ακέραια αριθμητική πρόοδος. Θεωρούμε την απεικόνιση $\varphi : I(P) \to Q$ με

$$\varphi(x_1, \dots, x_n) = a + x_1 q_1 + \cdots + x_n q_n. \tag{9.2.1}$$

Αφού η φ είναι περιορισμός αφινικής συνάρτησης από τον $\mathbb{Z}^n$ στο $\mathbb{Z}$, έπεται ότι η φ είναι ομομορφισμός Freiman τάξης h για κάθε $h \geqslant 2$.

Θεώρημα 9.2.1. *Έστω $h \geqslant 2$ και έστω $I(P)$ το ακέραιο παραλληλεπίπεδο διάστασης n που προσδιορίζεται από τους ακεραίους $\ell_1, \dots, \ell_n$. Τότε, υπάρχει n-διάστατη αριθμητική πρόοδος Q τέτοια ώστε τα $I(P)$ και Q να είναι Freiman ισομορφικά με τάξη h.*

Απόδειξη. Θεωρούμε έναν ακέραιο a και επιλέγουμε θετικούς ακεραίους $q_1, \dots, q_n$ τέτοιους ώστε

$$\sum_{j=1}^{k-1} h(\ell_j - 1) q_j < q_k \tag{9.2.2}$$

για $k = 2, \dots, n$. Θέτουμε

$$Q = Q(a; q_1, \dots, q_n; \ell_1, \dots, \ell_n).$$

Έστω $\varphi : I(P) \to Q$ η αφινική απεικόνιση που ορίζεται από την (9.2.1). Θα δείξουμε ότι η φ είναι ισομορφισμός Freiman τάξης h.

Έστω $x_i = (x_{i1}, \dots, x_{in}) \in I(P)$ και $y_i = (y_{i1}, \dots, y_{in}) \in I(P)$ για $i = 1, \dots, h$, και ας υποθέσουμε ότι

$$\varphi(x_1) + \cdots + \varphi(x_h) = \varphi(y_1) + \cdots + \varphi(y_h).$$

Τότε,

$$ha + \sum_{j=1}^{n} \sum_{i=1}^{h} x_{ij} q_j = ha + \sum_{j=1}^{n} \sum_{i=1}^{h} y_{ij} q_j.$$

Θέτουμε

$$w_j = \sum_{i=1}^{h} x_{ij} - \sum_{i=1}^{h} y_{ij}.$$

Τότε

$$|w_j| \leqslant h(\ell_j - 1)$$

και

$$\sum_{j=1}^{n} w_j q_j = 0.$$

Υποθέτουμε ότι υπάρχουν j ώστε $w_j \neq 0$, και έστω k ο μεγαλύτερος δείκτης για τον οποίον $w_k \neq 0$. Τότε,

$$-w_k q_k = \sum_{j=1}^{k-1} w_j q_j,$$

άρα

$$q_k \leqslant |w_k q_k| = \Big| \sum_{j=1}^{k-1} w_j q_j \Big| \leqslant \sum_{j=1}^{k-1} h(\ell_j - 1) q_j < q_k,$$

το οποίο είναι άτοπο. Συνεπώς, $w_j = 0$ για κάθε j. Έπεται ότι

$$x_1 + \cdots + x_h = y_1 + \cdots + y_h.$$

Άρα, κάθε n-διάστατο ακέραιο παραλληλεπίπεδο είναι Freiman ισόμορφο, με τάξη h, με μια n-διάστατη αριθμητική πρόοδο. □

Πόρισμα 9.2.2. *Έστω $h \geqslant 2$ και A πεπερασμένο σύνολο σημείων ενός πλέγματος. Τότε, το A είναι Freiman ισομορφικό, με τάξη h, με κάποιο σύνολο ακεραίων.*

Απόδειξη. Το A είναι υποσύνολο κάποιου n-διάστατου ακέραιου παραλληλεπιπέδου $I(P)$, και το $I(P)$ είναι Freiman ισόμορφο, με τάξη h, με κάποια n-διάστατη αριθμητική πρόοδο Q. Άρα, το A είναι Freiman ισόμορφο με την εικόνα του μέσω αυτού του ισομορφισμού. □

Πόρισμα 9.2.3. *Έστω $h \geqslant 2$ και A πεπερασμένο υποσύνολο μιας ομάδας που είναι ελεύθερη στρέψης. Τότε, το A είναι Freiman ισομορφικό, με τάξη h, με κάποιο σύνολο ακεραίων.*

Απόδειξη. Έστω G η ομάδα που παράγεται από το A. Αφού η G είναι πεπερασμένα παραγόμενη, από το Θεώρημα 7.5.5 έχουμε ότι η G είναι ισόμορφη με τον $\mathbb{Z}^n$ για κάποιον n, άρα υπάρχει ισομορφισμός Freiman τάξης h ανάμεσα στο A και κάποιο πεπερασμένο σύνολο ακεραίων σημείων. Από το Πόρισμα 9.2.2, αυτό το σύνολο είναι Freiman ισόμορφο, με τάξη h, με κάποιο σύνολο ακεραίων. □

Θεώρημα 9.2.4. *Έστω G και H αβελιανές ομάδες, και έστω Q μια n-διάστατη αριθμητική πρόοδος που περιέχεται στην G. Έστω $h \geqslant 2$. Αν $\varphi : Q \to H$ είναι ένας Freiman ομομορφισμός τάξης h, τότε το $\varphi(Q)$ είναι n-διάστατη αριθμητική πρόοδος στην H. Αν η $\varphi : Q \to \varphi(Q)$ είναι Freiman ισομορφισμός, τότε το Q είναι γνήσια n-διάστατη αριθμητική πρόοδος στην G αν και μόνο αν το $\varphi(Q)$ είναι επίσης γνήσια n-διάστατη αριθμητική πρόοδος στην H.*

Απόδειξη. Έστω $Q = \{a; q_1, \ldots, q_n; \ell_1, \ldots, \ell_n\}$. Ορίζουμε $a', q_1', \ldots, q_n' \in H$ θέτοντας

$$a' = \varphi(a) \quad \text{και} \quad q_i' = \varphi(a + q_i) - \varphi(a)$$

για $i = 1, \ldots, n$. Το σύνολο $Q' = \{a'; q_1', \ldots, q_n'; \ell_1, \ldots, \ell_n\}$ είναι n-διάστατη αριθμητική πρόοδος στην H. Θα δείξουμε ότι $Q' = \varphi(Q)$ και

$$\varphi(a + x_1q_1 + \cdots + x_nq_n) = a' + x_1q_1' + \cdots + x_nq_n'$$

για κάθε $a + x_1q_1 + \cdots + x_nq_n \in Q$.

Η απόδειξη θα γίνει με επαγωγή ως προς τον $m = \sum_{i=1}^n x_i$. Από τον ορισμό των $a', q_1', \ldots, q_n'$ βλέπουμε ότι το ζητούμενο ισχύει για $m = 0$ και $m = 1$. Ας υποθέσουμε ότι ισχύει για κάποιον $m \geqslant 1$. Έστω $r = a + x_1q_1 + \cdots + x_nq_n \in Q$ με $\sum_{i=1}^n x_i = m + 1$. Επιλέγουμε j τέτοιον ώστε $x_j \geqslant 1$ και θέτουμε $r' = r - q_j$. Από την επαγωγική υπόθεση έχουμε

$$\varphi(r') = a' + x_1q_1' + \cdots + x_{j-1}q_{j-1}' + (x_j - 1)q_j' + x_{j+1}q_{j+1}' + \cdots + x_nq_n'.$$

Αφού $r, a, r', a + q_j \in Q$ και

$$r + a = r' + (a + q_j),$$

και αφού κάθε ισομορφισμός Freiman τάξης h είναι και ισομορφισμός Freiman τάξης 2, έπεται ότι

$$\varphi(r) + \varphi(a) = \varphi(r') + \varphi(a + q_j).$$

Συνεπώς,

$$\varphi(r) = \varphi(r') + \varphi(a + q_j) - \varphi(a) = \varphi(r') + q'_j = a' + x_1 q'_1 + \cdots + x_n q'_n.$$

Έχουμε λοιπόν το ζητούμενο για κάθε $m \geqslant 0$, και $\varphi(Q) = Q'$. Αν η φ είναι ισομορφισμός Freiman τάξης h, τότε $|Q| = |\varphi(Q)|$, άρα η $\varphi(Q)$ είναι γνήσια αριθμητική πρόοδος αν και μόνο αν η Q είναι γνήσια. □

Θεώρημα 9.2.5. *Έστω $h' = h(k + \ell)$, όπου h, k και ℓ είναι θετικοί ακέραιοι. Έστω G και H αβελιανές ομάδες, και έστω $A \subseteq G$ και $B \subseteq H$ μη κενά, πεπερασμένα σύνολα που είναι Freiman ισομορφικά, τάξης h'. Τότε, τα σύνολα διαφορών $kA - \ell A$ και $kB - \ell B$ είναι Freiman ισομορφικά, τάξης h.*

Απόδειξη. Έστω $\varphi : A \to B$ ένας ισομορφισμός Freiman τάξης h', και έστω $\varphi^{(k)} : kA \to kB$, $\varphi^{(\ell)} : \ell A \to \ell B$ και $\varphi^{(k+\ell)} : (k + \ell)A \to (k + \ell)B$ οι απεικονίσεις που επάγονται από την φ. Αυτές οι απεικονίσεις είναι ένα προς ένα, και

$$\varphi^{(k+\ell)}(a_1 + \cdots + a_k + a_{k+1} + \cdots + a_{k+\ell}) = \varphi^{(k)}(a_1 + \cdots + a_k) + \varphi^{(\ell)}(a_{k+1} + \cdots + a_{k+\ell})$$

για κάθε $a_1, \ldots, a_{k+\ell} \in A$. Έστω $d \in kA - \ell A$. Αν

$$d = u - v = u' - v',$$

όπου $u, u' \in kA$ και $v, v' \in \ell A$, τότε

$$u + v' = u' + v \in (k + \ell)A.$$

Αφού η φ είναι ισομορφισμός Freiman τάξης $h' \geqslant k + \ell$, έπεται ότι

$$\varphi^{(k)}(u) + \varphi^{(\ell)}(v') = \varphi^{(k+\ell)}(u + v') = \varphi^{(k+\ell)}(u' + v) = \varphi^{(k)}(u') + \varphi^{(\ell)}(v),$$

άρα

$$\varphi^{(k)}(u) - \varphi^{(\ell)}(v) = \varphi^{(k)}(u') - \varphi^{(\ell)}(v').$$

Έπεται ότι η απεικόνιση $\psi : kA - \ell A \to kB - \ell B$ που ορίζεται από την

$$\psi(d) = \psi(u - v) = \varphi^{(k)}(u) - \varphi^{(\ell)}(v)$$

είναι καλά ορισμένη. Η ψ είναι επίσης επί διότι η φ είναι επί. Έστω $d = u - v \in kA - \ell A$ και $d' = u' - v' \in kA - \ell A$. Αν $\psi(d) = \psi(d')$, τότε

$$\varphi^{(k)}(u) - \varphi^{(\ell)}(v) = \varphi^{(k)}(u') - \varphi^{(\ell)}(v'),$$

άρα

$$\varphi^{(k+\ell)}(u + v') = \varphi^{(k+\ell)}(u' + v).$$

Έπεται ότι $u + v' = u' + v$, άρα $d = d'$. Αυτό δείχνει ότι η ψ είναι ένα προς ένα αντιστοιχία.

Θα δείξουμε ότι η ψ είναι ισομορφισμός Freiman τάξης h. Για $i = 1, \dots, h$, έστω $d_i, d_i' \in kA - \ell A$, και έστω ότι $d_i = u_i - v_i$ και $d_i' = u_i' - v_i'$, όπου $u_i, u_i' \in kA$ και $v_i, v_i' \in \ell A$. Τότε,

$$d_1 + \cdots + d_h = d_1' + \cdots + d_h'$$

αν και μόνο αν

$$u_1 + \cdots + u_h + v_1' + \cdots + v_h' = u_1' + \cdots + u_h' + v_1 + \cdots + v_h \in h(k+\ell)A,$$

αν και μόνο αν

$$\varphi^{(h(k+\ell))}(u_1 + \cdots + u_h + v_1' + \cdots + v_h') = \varphi^{(h(k+\ell))}(u_1' + \cdots + u_h' + v_1 + \cdots + v_h),$$

αν και μόνο αν

$$\begin{aligned}\varphi^{(k)}(u_1) + \cdots + \varphi^{(k)}(u_h) + \varphi^{(\ell)}(v_1') + \cdots + \varphi^{(\ell)}(v_h') \\ = \varphi^{(k)}(u_1') + \cdots + \varphi^{(k)}(u_h') + \varphi^{(\ell)}(v_1) + \cdots + \varphi^{(\ell)}(v_h),\end{aligned}$$

αν και μόνο αν

$$\psi(d_1) + \cdots + \psi(d_h) = \psi(d_1') + \cdots + \psi(d_h').$$

Αυτό αποδεικνύει ότι η ψ είναι ισομορφισμός Freiman τάξης h. □

9.3 Η μέθοδος του Bogolyubov

Έστω $m \geqslant 2$. Αν $x_i \equiv y_i \bmod m$ για κάθε $i = 1, \dots, n$, τότε

$$(x_1, \dots, x_n, m) = (y_1, \dots, y_n, m),$$

άρα ο «μέγιστος κοινός διαιρέτης» κλάσεων ισοτιμίας modulo m ορίζεται καλά. Για κάθε $x \in \mathbb{R}$ συμβολίζουμε με $\|x\|$ την απόσταση του x από τον πλησιέστερο ακέραιο. Έχουμε $\|x\| \leqslant 1/4$ αν και μόνο αν $\cos(2\pi x) \geqslant 0$ αν και μόνο αν $\mathrm{Re}(e^{2\pi i x}) \geqslant 0$. Αν $x, y \in \mathbb{Z}$ και $x \equiv y \bmod m$, τότε $\|x/m\| = \|y/m\|$. Έπεται ότι αυτή η συνάρτηση «απόστασης από τον πλησιέστερο ακέραιο» είναι καλά ορισμένη στις κλάσεις ισοτιμίας modulo m. Όμοια, η εκθετική συνάρτηση $e^{2\pi i x/m}$ είναι καλά ορισμένη στις κλάσεις ισοτιμίας modulo m. Αν $g \in \mathbb{Z}/m\mathbb{Z}$ και x είναι ένας ακέραιος στην κλάση ισοτιμίας g, ορίζουμε $\|g/m\| = \|x/m\|$ και $e^{2\pi i g/m} = e^{2\pi i x/m}$. Για $r_1, \dots, r_n \in \mathbb{Z}/m\mathbb{Z}$ και $\varepsilon > 0$, ορίζουμε την περιοχή Bohr

$$B(r_1, \dots, r_n; \varepsilon) = \Big\{ g \in \mathbb{Z}/m\mathbb{Z} : \Big\| \frac{g r_i}{m} \Big\| \leqslant \varepsilon \ \text{ για κάθε } \ i = 1, \dots, n \Big\}.$$

Παρατηρήστε ότι $B(0; \varepsilon) = \mathbb{Z}/m\mathbb{Z}$ για κάθε $\varepsilon > 0$.

Θεώρημα 9.3.1 (Bogolyubov)**.** *Έστω $m \geqslant 2$, και έστω A ένα μη κενό υποσύνολο του $\mathbb{Z}/m\mathbb{Z}$. Ορίζουμε $0 < \lambda \leqslant 1$ μέσω της $|A| = \lambda m$. Υπάρχει φυσικός αριθμός $n \leqslant \lambda^{-2}$ για τον οποίο υπάρχουν διακεκριμένες κλάσεις ισοτιμίας $r_1, r_2, \dots, r_n \in \mathbb{Z}/m\mathbb{Z}$ τέτοιες ώστε $r_1 = 0$ και*

$$B(r_1, \dots, r_n; 1/4) \subseteq 2A - 2A.$$

Απόδειξη. Θέτουμε $G = \mathbb{Z}/m\mathbb{Z}$. Για $r \in G$ θεωρούμε τον προσθετικό χαρακτήρα $\chi_r : G \to \mathbb{C}$ που ορίζεται από την

$$\chi_r(g) = e^{2\pi irg/m}.$$

Αυτή η συνάρτηση είναι καλά ορισμένη στις κλάσεις ισοτιμίας r και g modulo m, και $\chi_0(g) = 1$ για κάθε $g \in G$. Ορίζουμε

$$S_A(r) = \sum_{a\in A} \chi_r(a) = \sum_{a\in A} e^{2\pi ira/m}.$$

Τότε,

$$|S_A(r)| \leqslant S_A(0) = |A|$$

για κάθε $r \in G$, και

$$\sum_{r\in G} |S_A(r)|^2 = \sum_{r\in G} \sum_{a,a'\in A} e^{2\pi ir(a-a')/m} = |G|\,|A| = \frac{1}{\lambda}|A|^2.$$

Έστω $g \in G$. Τότε,

$$\sum_{r\in G} |S_A(r)|^4 \chi_r(g) = \sum_{g\in G} \sum_{a_1,a_2,a_3,a_4\in A} e^{2\pi ir(g-a_1-a_2+a_3+a_4)/m},$$

και αυτό το άθροισμα είναι μη μηδενικό αν και μόνο αν το g έχει τουλάχιστον αναπαράσταση της μορφής $g = a_1 + a_2 - a_3 - a_4$, δηλαδή, αν και μόνο αν το g ανήκει στο σύνολο διαφορών $2A - 2A$. Ορίζουμε

$$R_1 = \{r \in G : |S_A(r)| \geqslant \sqrt{\lambda}|A|\}$$

και

$$R_2 = \{r \in G : |S_A(r)| < \sqrt{\lambda}|A|\}.$$

Αφού $S_0 = |A| \geqslant \sqrt{\lambda}|A|$, έπεται ότι $0 \in R_1$ και $R_2 \neq G$. Συνεπώς,

$$\begin{aligned}\Big|\sum_{r\in R_2} |S_A(r)|^4\chi_r(g)\Big| &\leqslant \sum_{r\in R_2} |S_A(r)|^4 \leqslant \lambda|A|^2 \sum_{r\in R_2} |S_A(r)|^2 \\ &< \lambda|A|^2 \sum_{r\in G} |S_A(r)|^2 = \lambda|A|^2\,\frac{1}{\lambda}|A|^2 = |A|^4.\end{aligned}$$

Έστω $R_1 = \{r_1, r_2, \dots, r_n\}$, όπου $r_1 = 0$, και έστω $g \in B(r_1, \dots, r_n; 1/4)$. Τότε $\|r_i g/m\| \leqslant 1/4$ για $i = 1, \dots, n$, άρα

$$\mathrm{Re}(\chi_{r_i}(g)) = \mathrm{Re}(e^{2\pi ir_i g/m}) = \cos(2\pi r_i g/m) \geqslant 0.$$

Έπεται ότι

$$\begin{aligned}\mathrm{Re}\Big(\sum_{r\in G} |S_A(r)|^4\chi_r(g)\Big) &= \mathrm{Re}\Big(\sum_{r\in R_1} |S_A(r)|^4\chi_r(g)\Big) + \mathrm{Re}\Big(\sum_{r\in R_2} |S_A(r)|^4\chi_r(g)\Big) \\ &= |A|^4 + \sum_{r\in R_1\setminus\{0\}} |S_A(r)|^4\mathrm{Re}(\chi_r(g)) + \mathrm{Re}\Big(\sum_{r\in R_2} |S_A(r)|^4\chi_r(g)\Big) \\ &\geqslant |A|^4 + \mathrm{Re}\Big(\sum_{r\in R_2} |S_A(r)|^4\chi_r(g)\Big) \\ &\geqslant |A|^4 - \Big|\sum_{r\in R_2} |S_A(r)|^4\chi_r(g)\Big| > 0.\end{aligned}$$

Συνεπώς,

$$\sum_{r\in G}|S_A(r)|^4\chi_r(g)\neq 0$$

για κάθε $g\in B(r_1,\dots,r_n;1/4)$, άρα

$$B(r_1,\dots,r_n;1/4)\subseteq 2A-2A.$$

Τέλος, πρέπει να εκτιμήσουμε τον $n=|R_1|$. Αφού $|S_A(r)|\geqslant\sqrt{\lambda}|A|$ για κάθε $r\in R_1$, έπεται ότι

$$n\lambda|A|^2\leqslant\sum_{r\in R_1}|S_A(r)|^2\leqslant\sum_{r\in G}|S_A(r)|^2=\frac{1}{\lambda}|A|^2,$$

και έχουμε $n\leqslant\lambda^{-2}$. Αυτό ολοκληρώνει την απόδειξη. □

Θεώρημα 9.3.2. *Έστω $m\geqslant 2$, και έστω $R=\{r_1,\dots,r_n\}$ ένα σύνολο κλάσεων ισοτιμίας* mod m. *Αν $(r_1,\dots,r_n,m)=1$, τότε υπάρχει γνήσια n-διάστατη αριθμητική πρόοδος στο $\mathbb{Z}/m\mathbb{Z}$ η οποία περιέχεται στην Bohr περιοχή $B(r_1,\dots,r_n;1/4)$ και έχει πληθάριθμο*

$$|Q|>\frac{m}{(4n)^n}.$$

Απόδειξη. Θα χρησιμοποιήσουμε το Θεώρημα 7.5.7. Έστω $u=(u_1,\dots,u_n)$ και $v=(v_1,\dots,v_n)\in\mathbb{Z}^n$. Γράφουμε $u\equiv v$ mod m αν $u_i\equiv v_i$ mod m για κάθε $i=1,\dots,n$. Έστω M το πλέγμα των διανυσμάτων $v=(v_1,\dots,v_n)\in\mathbb{Z}^n$ για τα οποία $v\equiv 0$ mod m. Τότε, $M=(m\mathbb{Z})^n$ και $\det(M)=m^n$.

Θεωρούμε $r=(r_1,\dots,r_n)\in\mathbb{Z}^n$, όπου για $i=1,\dots,n$ συμβολίζουμε με r_i κάποιον σταθερό ακέραιο στην κλάση ισοτιμίας $r_i\in\mathbb{Z}/m\mathbb{Z}$. Τότε,

$$(r_1,\dots,r_n,m)=1. \tag{9.3.1}$$

Έστω Λ το σύνολο όλων των διανυσμάτων $u\in\mathbb{Z}^n$ για τα οποία $u\equiv qr$ mod m για κάποιον $q=0,1,\dots,m-1$. Τότε,

$$\Lambda=\bigcup_{q=0}^{m-1}(qr+M).$$

Το σύνολο Λ είναι πλέγμα, και το M είναι υποπλέγμα του Λ. Από την συνθήκη (9.3.1) βλέπουμε ότι τα m διανύσματα $0,r,2r,\dots,(m-1)r$ είναι ανά δύο ανισότιμα modulo m, άρα τα σύμπλοκα $(qr+M)$ είναι ανά δύο ξένα. Έπεται ότι ο δείκτης του M στο Λ είναι $[\Lambda:M]=m$ και, από το Θεώρημα 7.1.10,

$$\det(\Lambda)=\frac{\det(M)}{[\Lambda:M]}=m^{n-1}.$$

Έστω $K\subseteq\mathbb{R}^n$ ο κύβος που αποτελείται από όλα τα διανύσματα $(x_1,\dots,x_n)$ με $|x_i|<1/4$ για $i=1,\dots,n$. Το K είναι συμμετρικό κυρτό σώμα και $\mathrm{vol}(K)=1/2^n$. Έστω $\lambda_1,\dots,\lambda_n$ τα διαδοχικά ελάχιστα του K ως προς το πλέγμα Λ, και έστω $b_1,\dots,b_n$ ένα αντίστοιχο σύνολο γραμμικά ανεξάρτητων διανυσμάτων στο Λ. Τότε

$$b_i=(b_{i1},\dots,b_{in})\in\overline{\lambda_iK}\cap\Lambda$$

για $i = 1, \dots, n$. Από το δεύτερο θεώρημα του Minkowski (Θεώρημα 7.4.1) έπεται ότι

$$\lambda_1 \cdots \lambda_n \leqslant \frac{2^n \det(\Lambda)}{\mathrm{vol}(K)} = 4^n m^{n-1}.$$

Αφού

$$b_i \in \overline{\lambda_i K} = \Big\{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_i| \leqslant \frac{\lambda_i}{4}, \quad i = 1, \dots, n\Big\},$$

έχουμε

$$|b_{ij}| \leqslant \frac{\lambda_i}{4}$$

για κάθε $i, j = 1, \dots, n$. Αφού $b_i \in \Lambda$, έχουμε

$$b_i \equiv q_i r \bmod m$$

για κάποιον ακέραιο $q_i \in [0, m-1]$. Άρα,

$$b_{ij} \equiv q_i r_j \bmod m$$

για κάθε $i, j = 1, \dots, n$. Θέτουμε

$$\ell_i' = \Big[\frac{m}{n\lambda_i}\Big]$$

και

$$Q = \{x_1 q_1 + \cdots x_n q_n : -\ell_i' \leqslant x_i \leqslant \ell_i'\} \subseteq \mathbb{Z}/m\mathbb{Z}.$$

Θα δείξουμε ότι $Q \subseteq B(r_1, \dots, r_n; 1/4)$. Έστω $x = x_1 q_1 + \cdots + x_n q_n \in Q$. Τότε,

$$x r_j = \sum_{i=1}^n x_i q_i r_j \equiv \sum_{i=1}^n x_i b_{ij} \bmod m,$$

άρα

$$\begin{aligned}\Big\|\frac{x r_j}{m}\Big\| = \Big\|\sum_{i=1}^n \frac{x_i b_{ij}}{m}\Big\| &\leqslant \Big|\sum_{i=1}^n \frac{x_i b_{ij}}{m}\Big| \leqslant \sum_{i=1}^n \Big|\frac{x_i b_{ij}}{m}\Big| \leqslant \sum_{i=1}^n \frac{\ell_i' |b_{ij}|}{m} \leqslant \sum_{i=1}^n \frac{\ell_i' \lambda_i}{4m} \\ &\leqslant \sum_{i=1}^n \frac{1}{4n} = \frac{1}{4}.\end{aligned}$$

Αυτό σημαίνει ότι $x \in B$, άρα $Q \subseteq B$.

Στη συνέχεια δείχνουμε ότι το Q είναι γνήσια n-διάστατη αριθμητική πρόοδος. Έστω ότι

$$q_1 x_1 + \cdots + q_n x_n \equiv q_1 y_1 + \cdots + q_n y_n \bmod m,$$

όπου $-\ell_i' \leqslant x_i, y_i \leqslant \ell_i'$ για $i = 1, \dots, n$. Θέτουμε $z_i = x_i - y_i$. Τότε $|z_i| \leqslant 2\ell_i'$ και

$$\sum_{i=1}^n q_i z_i \equiv 0 \bmod m.$$

Έπεται ότι

$$\sum_{i=1}^n q_i r_j z_i \equiv \sum_{i=1}^n b_{ij} z_i \equiv 0 \bmod m$$

για $j = 1, \dots, n$. Αφού

$$\Big|\sum_{i=1}^{n} b_{ij} z_i\Big| \leqslant \sum_{i=1}^{n} |b_{ij}|\,|z_i| \leqslant \sum_{i=1}^{n} \frac{\lambda_i}{4} \cdot 2\ell_i' \leqslant \sum_{i=1}^{n} \frac{m}{2n} < m,$$

έπεται ότι $\sum_{i=1}^{n} b_{ij} z_i = 0$ για $j = 1, \dots, n$, άρα

$$\sum_{i=1}^{n} z_i b_i = 0.$$

Αφού τα διανύσματα b_i είναι γραμμικά ανεξάρτητα, συμπεραίνουμε ότι $z_i = 0$ για κάθε i, άρα

$$|Q| = (2\ell_1' + 1) \cdots (2\ell_n' + 1).$$

Ορίζουμε $\ell_i = 2\ell_i' + 1$ και $a = -\sum_{i=1}^{n} \ell_i' q_i$. Τότε, το Q είναι η γνήσια n-διάστατη αριθμητική πρόοδος

$$Q(a; q_1, \dots, q_n; \ell_1, \dots, \ell_n).$$

Επιπλέον,

$$|Q| = \ell_1 \cdots \ell_n \geqslant \prod_{i=1}^{n} (\ell_i' + 1) > \prod_{i=1}^{n} \frac{m}{n\lambda_i} = \Big(\frac{m}{n}\Big)^n \Big(\prod_{i=1}^{n} \lambda_i\Big)^{-1} \geqslant \Big(\frac{m}{n}\Big)^n (4^n m^{n-1})^{-1} = \frac{m}{(4n)^n}.$$

Αυτό ολοκληρώνει την απόδειξη. □

Θεώρημα 9.3.3. *Έστω p πρώτος αριθμός, και έστω R ένα μη κενό σύνολο κλάσεων ισοτιμίας* $\bmod p$ *με $|R| = \lambda p$. Υπάρχει φυσικός αριθμός $n \leqslant \lambda^{-2}$ για τον οποίο υπάρχει γνήσια n-διάστατη αριθμητική πρόοδος Q τέτοια ώστε*

$$Q \subseteq 2R - 2R$$

και

$$\ell(Q) = |Q| > \delta p,$$

όπου

$$\delta = \frac{1}{(4n)^n} \geqslant \Big(\frac{\lambda^2}{4}\Big)^{1/\lambda^2}.$$

Απόδειξη. Αν $\mathbb{Z}/p\mathbb{Z} = 2R - 2R$, θέτουμε $n = 1$ και θεωρούμε την μονοδιάστατη αριθμητική πρόοδο $Q = Q(0; 1; p) = \mathbb{Z}/p\mathbb{Z}$. Τότε $Q \subseteq 2R - 2R$ και $|Q| = p > \delta p$, όπου

$$\delta = \frac{1}{4} \geqslant \Big(\frac{\lambda^2}{4}\Big)^{1/\lambda^2}$$

για κάθε $\lambda \in (0, 1]$.

Έστω τώρα ότι $2R - 2R \neq \mathbb{Z}/p\mathbb{Z}$. Από το Θεώρημα 9.3.1, για κάποιον θετικό ακέραιο $n \leqslant \lambda^{-2}$ υπάρχουν διακεκριμένες κλάσεις ισοτιμίας $r_1, r_2, \dots, r_n$ modulo p τέτοιες ώστε $r_1 = 0$ και

$$B = B(r_1, \dots, r_n; 1/4) \subseteq 2R - 2R.$$

Αφοού $B(0; 1/4) = \mathbb{Z}/p\mathbb{Z}$, αναγκαστικά έχουμε $n \geqslant 2$, άρα

$$(r_1, \dots, r_n, p) = 1.$$

Από το Θεώρημα 9.3.2, υπάρχει γνήσια n-διάστατη αριθμητική πρόοδος Q τέτοια ώστε $Q \subseteq B$ και $|Q| > \delta p$, όπου

$$\delta = \frac{1}{(4n)^n} \geqslant \left(\frac{\lambda^2}{4}\right)^{1/\lambda^2}.$$

Αυτό ολοκληρώνει την απόδειξη. □

9.4 Το θεώρημα του Ruzsa

Θεώρημα 9.4.1 (Ruzsa). *Έστω W ένα πεπερασμένο σύνολο ακεραίων. Έστω $h \geqslant 2$ και*

$$D = D_{h,h}(W) = hW - hW.$$

Για κάθε

$$m \geqslant 4h|D_{h,h}(W)| = 4h|D|$$

υπάρχει σύνολο $W' \subseteq W$ τέτοιο ώστε

$$|W'| \geqslant \frac{|W|}{h}$$

το οποίο είναι Freiman ισομορφικό, τάξης h, με ένα σύνολο κλάσεων ισοτιμίας mod n.

Απόδειξη. Έστω $m \geqslant 4h|D|$, και έστω p πρώτος αριθμός τέτοιος ώστε

$$p > \max\{m, 2h \max_{w \in W} |w|\}.$$

Έστω $1 \leqslant q \leqslant p-1$. Θα κατασκευάσουμε μια απεικόνιση $\varphi_q : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, και στη συνέχεια θα δείξουμε ότι για κάποιον q υπάρχει υποσύνολο W' του W τέτοιο ώστε $|W'| \geqslant |W|/h$ και η φ_q περιορισμένη στο W' είναι ισομορφισμός Freiman τάξης h. Η απεικόνιση φ_q θα είναι σύνθεση τεσσάρων απεικονίσεων:

$$\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}/p\mathbb{Z} \xrightarrow{\beta_q} \mathbb{Z}/p\mathbb{Z} \xrightarrow{\gamma} \mathbb{Z} \xrightarrow{\delta} \mathbb{Z}/m\mathbb{Z},$$

για κατάλληλες α, β_q, γ και δ που θα οριστούν παρακάτω.

Έστω $\alpha : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ η φυσιολογική απεικόνιση που στέλνει το w στο $w + p\mathbb{Z}$. Αφού η α είναι ομομορφισμός ομάδων, είναι ομομορφισμός Freiman τάξης h. Παρόλο που δεν είναι ισομορφισμός ομάδων, μπορούμε να δείξουμε ότι η α περιορισμένη στο W είναι ισομορφισμός Freiman τάξης h. Έστω $w_1, \ldots, w_h, w'_1, \ldots, w'_h \in W$, και ας υποθέσουμε ότι

$$\alpha(w_1) + \cdots + \alpha(w_h) = \alpha(w'_1) + \cdots + \alpha(w'_h).$$

Τότε

$$\alpha(w_1 + \cdots + w_h) = \alpha(w'_1 + \cdots + w'_h),$$

άρα

$$(w_1 + \cdots + w_h) - (w'_1 + \cdots + w'_h) \equiv 0 \bmod p.$$

Αφού

$$|(w_1 + \cdots + w_h) - (w'_1 + \cdots + w'_h)| \leqslant 2h \max_{w \in W} |w| < p,$$

έπεται ότι

$$(w_1 + \cdots + w_h) - (w'_1 + \cdots + w'_h) = 0.$$

Συνεπώς, η $\alpha : W \to \alpha(W) \subseteq \mathbb{Z}/p\mathbb{Z}$ είναι ισομορφισμός Freiman τάξης h.

Για $1 \leqslant q \leqslant p-1$, έστω $\beta_q : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ η απεικόνιση που στέλνει το $w + p\mathbb{Z}$ στο $wq + p\mathbb{Z}$. Αφού η β_q είναι ισομορφισμός ομάδων, είναι ισομορφισμός Freiman τάξης h σε κάθε υποσύνολο του $\mathbb{Z}/p\mathbb{Z}$.

Έστω $\gamma : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}$ η απεικόνιση που στέλνει το $w + p\mathbb{Z}$ στον ελάχιστο μη αρνητικό αντιπρόσωπό του. Η εικόνα της γ είναι το διάστημα ακεραίων $[0, p-1]$. Η απεικόνιση γ δεν είναι ομομορφισμός ομάδων ούτε ομομορφισμός Freiman τάξης h. Μπορούμε όμως να γράψουμε το $\mathbb{Z}/p\mathbb{Z}$ ως ένωση h υποσυνόλων έτσι ώστε ο περιορισμός της γ σε καθένα από αυτά τα υποσύνολα να είναι ισομορφισμός Freiman τάξης h. Για $i = 1, \ldots, h$, θέτουμε

$$U_i = \gamma^{-1}\Big[\frac{(i-1)(p-1)}{h}, \frac{i(p-1)}{h}\Big] \subseteq \mathbb{Z}/p\mathbb{Z}.$$

Αφού

$$[0, p-1] = \bigcup_{i=1}^{h} \Big[\frac{(i-1)(p-1)}{h}, \frac{i(p-1)}{h}\Big],$$

έπεται ότι

$$\mathbb{Z}/p\mathbb{Z} = \bigcup_{i=1}^{h} U_i.$$

Σταθεροποιούμε το σύνολο U_i, και θεωρούμε $u_j + p\mathbb{Z} \in U_i$ και $u'_j + p\mathbb{Z} \in U_i$ για $j = 1, \ldots, h$. Αν

$$u_1 + \cdots + u_h + p\mathbb{Z} = u'_1 + \cdots + +u'_h + p\mathbb{Z}$$

στο $\mathbb{Z}/p\mathbb{Z}$, τότε

$$\gamma(u_1 + p\mathbb{Z}) + \cdots + \gamma(u_h + p\mathbb{Z}) \equiv \gamma(u'_1 + p\mathbb{Z}) + \cdots + \gamma(u'_h + p\mathbb{Z}) \bmod p$$

στο $\mathbb{Z}$. Αφού

$$\gamma(u_1 + p\mathbb{Z}) + \cdots + \gamma(u_h + p\mathbb{Z}) \in [(i-1)(p-1), i(p-1)]$$

και

$$\gamma(u'_1 + p\mathbb{Z}) + \cdots + \gamma(u'_h + p\mathbb{Z}) \in [(i-1)(p-1), i(p-1)],$$

έπεται ότι

$$|(\gamma(u_1 + p\mathbb{Z}) + \cdots + \gamma(u_h + p\mathbb{Z})) - (\gamma(u'_1 + p\mathbb{Z}) + \cdots + \gamma(u'_h + p\mathbb{Z}))| \leqslant p - 1,$$

άρα

$$\gamma(u_1 + p\mathbb{Z}) + \cdots + \gamma(u_h + p\mathbb{Z}) = \gamma(u'_1 + p\mathbb{Z}) + \cdots + \gamma(u'_h + p\mathbb{Z}).$$

Άρα, η γ είναι ομομορφισμός Freiman τάξης h. Αντίστροφα, αν

$$\gamma(u_1 + p\mathbb{Z}) + \cdots + \gamma(u_h + p\mathbb{Z}) = \gamma(u'_1 + p\mathbb{Z}) + \cdots + \gamma(u'_h + p\mathbb{Z})$$

στο $\mathbb{Z}$, τότε

$$u_1 + \cdots + u_h + p\mathbb{Z} = u'_1 + \cdots + +u'_h + p\mathbb{Z}$$

στο $\mathbb{Z}/p\mathbb{Z}$, άρα η γ περιορισμένη σε κάθε σύνολο U_i είναι ισομορφισμός Freiman τάξης h.

Θέτουμε

$$W_{i,q} = W \cap \alpha^{-1}(\beta_q^{-1}(U_i))$$

για $i = 1, \dots, h$. Τότε

$$W = \bigcup_{i=1}^{h} W_{i,q},$$

άρα

$$|W_{j,q}| \geqslant \frac{|W|}{h}$$

για κάποιον j. Έστω $W'_q = W_{j,q}$. Ορίζουμε $\vartheta_q : W \to \mathbb{Z}$ με $\vartheta_q = \gamma \circ \beta_q \circ \alpha$. Τότε,

$$\vartheta_q(w) = wq - \Big[\frac{wq}{p}\Big]p \in [0, p-1]$$

για κάθε $a \in W$. Αν

$$V_q = \vartheta_q(W)$$

και

$$V'_q = \vartheta_q(W'_q),$$

τότε η $\vartheta_q : W'_q \to V - q'$ είναι ισομορφισμός Freiman τάξης h.

Έστω $\delta : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ η φυσιολογική απεικόνιση που στέλνει το w στο $w + m\mathbb{Z}$. Η δ είναι ισομορφισμός Freiman τάξης h. Θα αποδείξουμε ότι υπάρχει τουλάχιστον ένας $q \in [1, p-1]$ τέτοιος ώστε ο περιορισμός της δ στο V_q να είναι ισομορφισμός Freiman τάξης h.

Θεωρούμε $q \in [1, p-1]$ και υποθέτουμε ότι η $\delta : V_q \to \mathbb{Z}/m\mathbb{Z}$ δεν είναι ισομορφισμός Freiman τάξης h. Τότε υπάρχουν ακέραιοι $v_1, \dots, v_h, v'_1, \dots, v'_h \in V_q \subseteq [0, p-1]$ τέτοιοι ώστε

$$v_1 + \cdots + v_h \neq v'_1 + \cdots + v'_h$$

αλλά

$$\delta(v_1 + \cdots + v_h) = \delta(v_1) + \cdots + \delta(v_h) = \delta(v'_1) + \cdots + \delta(v'_h) = \delta(v'_1 + \cdots + v'_h).$$

Ορίζουμε

$$v^* = (v_1 + \cdots + v_h) - (v'_1 + \cdots + v'_h).$$

Αφού $m > 4h|D|$, έχουμε

$$|v^*| \leqslant h(p-1) < hp < mp \tag{9.4.1}$$

και

$$v^* \equiv 0 \bmod m \tag{9.4.2}$$

αλλά

$$v^* \neq 0. \tag{9.4.3}$$

Επιλέγουμε $w_i, w_i' \in W$ τέτοιους ώστε $\vartheta_q(w_i) = v_i$ και $\vartheta_q(w_i') = v_i'$ για κάθε $i = 1, \dots, h$. Ορίζουμε

$$w^* = (w_1 + \cdots + w_h) - (w_1' + \cdots + w_h').$$

Τότε, $w^* \in D = hW - hW$. Για $i = 1, \dots, h$,

$$v_i \equiv w_i q \bmod p$$

και

$$v_i' \equiv w_i' q \bmod p.$$

Άρα,

$$v^* \equiv w^* q \bmod p$$

και συνεπώς

$$v^* = \gamma(w^* q + p\mathbb{Z}) + xp \tag{9.4.4}$$

για κάποιον ακέραιο x. Αν $w^* \equiv 0 \bmod p$, τότε

$$v^* \equiv 0 \bmod p. \tag{9.4.5}$$

Αφού ο p είναι πρώτος και $1 < m < p$, έχουμε $(m, p) = 1$. Τότε, από τις ισοτιμίες (9.4.2) και (9.4.5) βλέπουμε ότι

$$v^* \equiv 0 \bmod mp.$$

Αφού $|v^*| < mp$ από την (9.4.1), έπεται ότι $v^* = 0$, το οποίο είναι άτοπο από την (9.4.3). Συνεπώς,

$$w^* \not\equiv 0 \bmod p.$$

Ο $\gamma(w^* q + p\mathbb{Z})$ είναι ο μικρότερος μη αρνητικός ακέραιος στην κλάση ισοτιμίας $w^* q + p\mathbb{Z}$. Από τις (9.4.2) και (9.4.4),

$$v^* = \gamma(w^* q + p\mathbb{Z}) + xp \equiv 0 \bmod m,$$

και από την ανισότητα (9.4.1) έπεται ότι

$$-h \leqslant x \leqslant h - 1.$$

Άρα, αν $q \in [1, p-1]$ και η $\delta : V_q \to \mathbb{Z}/m\mathbb{Z}$ δεν είναι ισομορφισμός Freiman τάξης h, τότε υπάρχουν ακέραιοι $w^* \in D$ και $x \in [-h, h-1]$ τέτοιοι ώστε $w^* \not\equiv 0 \bmod p$ και

$$\gamma(w^* q + p\mathbb{Z}) + xp \equiv 0 \bmod m. \tag{9.4.6}$$

Μετράμε το πλήθος των τριάδων (q, w^*, x) που ικανοποιούν αυτές τις συνθήκες. Επιλέγουμε έναν ακέραιο $x \in [-h, h-1]$. Υπάρχουν $2h$ τέτοιες επιλογές. Αφού $p > m$, η ισοτιμία

$$y + xp \equiv 0 \bmod m$$

έχει το πολύ

$$\frac{p-1}{m} + 1 \leqslant \frac{2(p-1)}{m}$$

λύσεις $y \in [1, p-1]$. Επιλέγουμε έναν ακέραιο $w^* \in D$ τέτοιον ώστε $w^* \not\equiv 0 \bmod p$. Αφού $0 \in D$, υπάρχουν το πολύ $|D|-1$ τέτοιες επιλογές. Αφού $w^* \not\equiv 0 \bmod p$, για κάθε ακέραιο $y \in [1, p-1]$ υπάρχει μοναδικός ακέραιος $q \in [1, p-1]$ τέτοιος ώστε $y = \gamma(w^* q + p\mathbb{Z})$. Έτσι, για κάθε ζεύγος επιτρεπτών x και w^* υπάρχουν το πολύ $2(p-1)/m$ επιλογές του $q \in [1, p-1]$ έτσι ώστε η τριάδα (q, w^*, x) να μας δίνει λύση της ισοτιμίας (9.4.6). Αφού $m \geqslant 4h|D|$, το πλήθος των τριάδων είναι το πολύ

$$2h \cdot \frac{2(p-1)}{m} \cdot (|D|-1) < \frac{4h|D|(p-1)}{m} \leqslant p-1.$$

Συνεπώς, υπάρχει τουλάχιστον ένας ακέραιος $q \in [1, p-1]$ ο οποίος δεν εμφανίζεται σε καμία από τις τριάδες, και γι' αυτόν τον q η απεικόνιση

$$\delta : V_q = \vartheta_q(W) \to \mathbb{Z}/m\mathbb{Z}$$

είναι ισομορφισμός Freiman τάξης h. Έστω $W' = W'_q$. Αφού η

$$\vartheta_q : W' \to V'_q \subseteq V_q \subseteq \mathbb{Z}$$

είναι επίσης ισομορφισμός Freiman τάξης h, έπεται ότι υπάρχει ισομορφισμός Freiman τάξης h από το W' στο $\mathbb{Z}/m\mathbb{Z}$. Επιπλέον, $|W'| \geqslant |W|/h$, και η απόδειξη είναι πλήρης. □

Θεώρημα 9.4.2. *Έστω c, c_1 και c_2 θετικοί πραγματικοί αριθμοί. Έστω $k \geqslant 1$, και έστω A και B πεπερασμένα υποσύνολα μιας αβελιανής ομάδας ελεύθερης στρέψης, τέτοια ώστε*

$$c_1 k \leqslant |A|, |B| \leqslant c_2 k$$

και

$$|A+B| \leqslant ck.$$

Τότε, το A περιέχεται σε n-διάστατη αριθμητική πρόοδο μήκους το πολύ ℓk, όπου οι n και ℓ εξαρτώνται μόνο από τις σταθερές c, c_1 και c_2.

Απόδειξη. Έστω G η ομάδα που παράγεται από το A. Αφού η G είναι πεπερασμένα παραγόμενη αβελιανή ομάδα ελεύθερη στρέψης, εφαρμόζοντας το Πόρισμα 9.2.3 με $h = 32$ βλέπουμε ότι υπάρχει ισομορφισμός Freiman τάξης 32 ανάμεσα στο A και κάποιο σύνολο W ακεραίων. Αφού $32 = 2(8+8)$, το Θεώρημα 9.2.5 μας δίνει ότι τα σύνολα διαφορών $D_{8,8}(A) = 8A - 8A$ και $D_{8,8}(W) = 8W - 8W$ είναι Freiman ισόμορφα τάξης 2, άρα $|D_{8,8}(W)| = |D_{8,8}(A)|$. Θέτουμε $c_3 = c/c_1$. Αφού

$$|A+B| \leqslant ck \leqslant (c/c_1)|A| = c_3|A|,$$

από το Θεώρημα 8.2.2 συμπεραίνουμε ότι

$$|D_{8,8}(W)| = |D_{8,8}(A)| \leqslant c_3^{16}|A| = c_3^{16}|W|.$$

Τώρα χρησιμοποιούμε το αίτημα του Bertrand το οποίο ισχυρίζεται ότι για κάθε θετικό ακέραιο n υπάρχει πρώτος αριθμός p μεταξύ n και $2n$. Θέτουμε $n = 32|D_{8,8}(W)|$. Υπάρχει πρώτος p τέτοιος ώστε

$$|W| < 32|W| \leqslant 32|D_{8,8}(W)| < p < 64|D_{8,8}(W)| \leqslant 64c_3^{16}|W|.$$

Εφαρμόζοντας το Θεώρημα 9.4.1 με $h = 8$ βρίσκουμε σύνολο $W' \subseteq W$ τέτοιο ώστε $|W'| \geqslant |W|/8$, το οποίο είναι Freiman ισόμορφο, με τάξη 8, με ένα σύνολο R κλάσεων ισοτιμίας modulo p. Ορίζουμε $\lambda \in (0,1]$ μέσω της $\lambda p = |R|$. Τότε,

$$\lambda p = |R| = |W'| \geqslant \frac{|W|}{8} > \frac{p}{8 \cdot 64 c_3^{16}},$$

άρα

$$\lambda > 2^{-9} c_3^{-16}.$$

Από το Θεώρημα 9.3.3, το σύνολο διαφορών $2R - 2R$ περιέχει γνήσια n_1-διάστατη αριθμητική πρόοδο Q' μήκους

$$\ell(Q') = |Q'| > \delta p > \delta |W| = \delta |A|,$$

όπου

$$n_1 \leqslant \lambda^{-2} < 2^{18} c_3^{32}$$

και

$$\delta = (4n_1)^{-n_1} > (2^{20} c_3^{32})^{-2^{18} c_3^{32}}.$$

Αφού $8 = 2(2+2)$, από το Θεώρημα 9.2.5 βλέπουμε ότι τα σύνολα διαφορών $2R - 2R$ και $2W' - 2W'$ είναι Freiman ισόμορφα με τάξη 2.

Τα σύνολα W και A είναι Freiman ισόμορφα με τάξη 32, άρα και με τάξη 8. Έστω A' η εικόνα του W' μέσω αυτού του ισομορφισμού. Από το Θεώρημα 9.2.5, τα σύνολα διαφορών $2W' - 2W'$ και $2A' - 2A'$ είναι Freiman ισόμορφα με τάξη 2, άρα τα $2R - 2R$ και $2A' - 2A'$ είναι Freiman ισόμορφα. Έστω Q_1 η εικόνα του Q' μέσω αυτού του ισομορφισμού. Από το Θεώρημα 9.2.4, το Q_1 είναι γνήσια n_1-διάστατη αριθμητική πρόοδος τέτοια ώστε

$$Q_1 \subseteq 2A' - 2A' \subseteq 2A - 2A \subseteq G$$

και

$$\delta |A| < |Q'| = |Q_1| = \ell(Q_1) \leqslant |2A - 2A| \leqslant c_3^4 |A|.$$

Έστω $A^* = \{a_1, \ldots, a_{n_2}\}$ ένα μεγιστικό σύνολο στοιχείων του A τέτοιο ώστε τα σύνολα $a_i + Q_1$ να είναι ανά δύο ξένα. Αφού

$$\bigcup_{i=1}^{n_2} (a_i + Q_1) = A^* + Q_1 \subseteq A + Q_1 \subseteq 3A - 2A,$$

από το Θεώρημα 8.2.2 βλέπουμε ότι

$$n_2 |Q_1| = \sum_{i=1}^{n_2} |a_i + Q_1| = \Big| \bigcup_{i=1}^{n_2} (a_i + Q_1) \Big| = |A^* + Q_1| \leqslant |3A - 2A| \leqslant c_3^5 |A|.$$

Άρα,

$$n_2 \leqslant \frac{c_3^5 |A|}{|Q_1|} < \frac{c_3^5 |A|}{\delta |A|} = c_3^5 (4n_1)^{n_1}.$$

Το A^* είναι υποσύνολο της n_2-διάστατης αριθμητικής προόδου

$$Q_2 = \{x_1 a_1 + \cdots + + x_{n_2} a_{n_2} : 0 \leqslant x_i < 2\}$$

που έχει μήκος $\ell(Q_2) = 2^{n_2}$. Αφού το A^* είναι μεγιστικό, για κάθε $a \in A$ υπάρχει $a_i \in A^*$ τέτοιο ώστε

$$(a + Q_1) \cap (a_i + Q_1) \neq \emptyset,$$

άρα υπάρχουν ακέραιοι $q, q' \in Q_1$ τέτοιοι ώστε $a + q = a_i + q'$. Τότε,

$$a = a_i + q' - q \in A^* + Q_1 - Q_1 \subseteq Q_2 + Q_1 - Q_1.$$

Θέτουμε $Q = Q_2 + Q_1 - Q_1$. Τότε

$$A \subseteq Q.$$

Από το Θεώρημα 9.1.2, το $Q_1 - Q_1$ είναι n_1-διάστατη αριθμητική πρόοδος μήκους

$$\ell(Q_1 - Q_1) < 2^{n_1}\ell(Q_1) \leqslant 2^{n_1}c_3^4|A| \leqslant 2^{n_1}(c/c_1)^4c_2k,$$

άρα το $Q = Q_2 + (Q_1 - Q_1)$ είναι αριθμητική πρόοδος διάστασης $n = n_1 + n_2$ και μήκους

$$\ell = \ell(Q) \leqslant \ell(Q_2)\ell(Q_1 - Q_1) < 2^{n_2}2^{n_1}(c/c_1)^4c_2k = 2^n(c/c_1)^4c_2k,$$

με τους n και ℓ να εξαρτώνται μόνο από τις σταθερές c, c_1 και c_2. □

Το θεώρημα του Freiman είναι ειδική περίπτωση του προηγούμενου θεωρήματος: αρκεί να πάρουμε A ένα πεπερασμένο σύνολο ακεραίων και $B = A$.

9.5 Μικρά αθροίσματα συνόλων και αριθμητικές πρόοδοι μεγάλου μήκους

Σε αυτήν την παράγραφο παρουσιάζουμε μια εφαρμογή του θεωρήματος του Freiman. Θα δείξουμε ότι αν A είναι ένα αρκετά μεγάλο σύνολο ακεραίων (ή, γενικότερα, στοιχείων μιας ελεύθερης στρέψης αβελιανής ομάδας) τέτοιο ώστε $|2A| \leqslant c|A|$ τότε το A περιέχει αρκετά μεγάλη αριθμητική πρόοδο. Η ακριβής διατύπωση είναι η ακόλουθη.

Θεώρημα 9.5.1. *Έστω $c \geqslant 2$ και $t \geqslant 3$. Υπάρχει ακέραιος $k_0(c,t)$ τέτοιος ώστε αν A είναι ένα υποσύνολο μιας ελεύθερης στρέψης αβελιανής ομάδας G με $|A| \geqslant k_0(c,t)$ και $|2A| \leqslant c|A|$, τότε το A περιέχει μια αριθμητική πρόοδο μήκους μεγαλύτερου ή ίσου από t.*

Θα χρησιμοποιήσουμε το διάσημο θεώρημα του Szemerédi το οποίο ισχυρίζεται ότι για κάθε $\delta > 0$ και $t \geqslant 3$ υπάρχει φυσικός $\ell_0(\delta, t)$ τέτοιος ώστε αν $\ell \geqslant \ell_0(\delta, t)$ και A είναι ένα υποσύνολο του $[0, \ell - 1]$ με $|A| \geqslant \delta\ell$, τότε το A περιέχει αριθμητική πρόοδο μήκους t. Από αυτό έπεται το επόμενο λήμμα.

Λήμμα 9.5.2. *Έστω $\delta > 0$ και $t \geqslant 3$. Υπάρχει φυσικός $\ell_0(\delta, t)$ τέτοιος ώστε αν Q είναι μια αριθμητική πρόοδος μήκους ℓ σε μια ελεύθερη στρέψης αβελιανή ομάδα G και B είναι ένα υποσύνολο του Q με $|B| \geqslant \delta\ell$ και $\ell \geqslant \ell_0(\delta, t)$ τότε το B περιέχει αριθμητική πρόοδο μήκους t.*

Απόδειξη. Έστω $\ell_0(\delta, t)$ ο φυσικός που μας δίνει το θεώρημα του Szemerédi. Αφού το Q είναι μονοδιάστατη αριθμητική πρόοδος, υπάρχουν a και $q \neq 0$ στην G τέτοια ώστε

$$Q = \{a + xq : 0 \leqslant x < \ell\}.$$

Έστω

$$A = \{x \in [0, \ell - 1] : a + xq \in B\}.$$

Τότε, το A είναι σύνολο ακεραίων, και $|A| = |B| \geqslant \delta\ell$. Από το θεώρημα του Szemerédi, το A περιέχει μια αριθμητική πρόοδο μήκους t, άρα υπάρχουν ακέραιοι a' και $q' \neq 0$ τέτοιοι ώστε $a' + yq' \in A$ για κάθε $0 \leqslant y < t$. Θέτουμε $a'' = a + a'q$ και $q'' = q'q$. Τότε $q'' \neq 0$ γιατί η G είναι ελεύθερη στρέψης, και

$$a + (a' + yq')q = a'' + yq'' \in B$$

για κάθε $0 \leqslant y < t$. Συνεπώς, το B περιέχει αριθμητική πρόοδο μήκους t. □

Απόδειξη του Θεωρήματος 9.5.1. Θέτουμε $k = |A|$. Από το θεώρημα του Freiman υπάρχουν ακέραιοι $n = n(c)$ και $\ell = \ell(c)$ τέτοιοι ώστε το A να περιέχεται σε μια n-διάστατη αριθμητική πρόοδο Q μήκους

$$\ell(Q) \leqslant \ell k.$$

Έστω

$$Q = \{a + x_1q_1 + \cdots + x_nq_n : 0 \leqslant x_i < \ell_i, \text{ για } i = 1, \ldots, n\}.$$

Τότε,

$$\ell(Q) = \ell_1\ell_2 \cdots \ell_n.$$

Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $\ell_1 \leqslant \ell_2 \leqslant \cdots \leqslant \ell_n$. Έπεται ότι

$$k = |A| \leqslant |Q| \leqslant \ell(Q) = \ell_1\ell_2 \cdots \ell_n \leqslant \ell_n^n,$$

άρα

$$\ell_n \geqslant \sqrt[n]{k}.$$

Έστω Y το σύνολο των ακεραίων σημείων $y = (y_1, \ldots, y_{n-1}) \in \mathbb{Z}^{n-1}$ για τα οποία ισχύει $0 \leqslant y_i < \ell_i$ για κάθε $i = 1, \ldots, n-1$. Τότε,

$$|Y| = \ell_1\ell_2 \cdots \ell_{n-1}.$$

Για κάθε $y \in Y$, το σύνολο

$$L(y) = \{a + y_1q_1 + \cdots + y_{n-1}q_{n-1} + x_nq_n : 0 \leqslant x_n < \ell_n\}$$

είναι αριθμητική πρόοδος μήκους ℓ_n στην G. Αφού

$$A \subseteq Q = \bigcup_{y \in Y} L(y),$$

έπεται ότι

$$A = \bigcup_{y \in Y} (L(y) \cap A),$$

άρα

$$k = |A| \leqslant \sum_{y \in Y} |L(y) \cap A|.$$

Μπορούμε να δώσουμε ένα κάτω φράγμα για τον μέσο πληθάριθμο των τομών των αριθμητικών προόδων $L(y)$ με το σύνολο A ως εξής:

$$\frac{1}{|Y|} \sum_{y \in Y} |L(y) \cap A| \geqslant \frac{k}{\ell_1 \cdots \ell_{n-1}} \geqslant \frac{\ell_n}{\ell} \geqslant \frac{\sqrt[n]{k}}{\ell}.$$

Έπεται ότι υπάρχει κάποιο $y \in Y$ τέτοιο ώστε

$$|L(y) \cap A| \geqslant \frac{\sqrt[n]{k}}{\ell}.$$

Θέτουμε

$$k_0(c,t) = \ell_0(1/\ell, t)^n,$$

όπου $\ell_0(1/\ell, t)$ είναι ο φυσικός που προσδιορίζεται από το Λήμμα 9.5.2. Αν $|A| = k \geqslant k_0(c,t)$ τότε το $L(y)$ είναι αριθμητική πρόοδος μήκους

$$\ell_n \geqslant \sqrt[n]{k} \geqslant \sqrt[n]{k_0(c,t)} = \ell_0(1/\ell, t),$$

άρα το $L(y) \cap A$ περιέχει αριθμητική πρόοδο με μήκος μεγαλύτερο ή ίσο από t. Αυτό ολοκληρώνει την απόδειξη. □

ΠΑΡΑΡΤΗΜΑ A

A.1 Άθροιση κατά μέρη

Θεώρημα A.1.1 (άθροιση κατά μέρη)**.** *Έστω $u(n)$ και $f(n)$ αριθμητικές συναρτήσεις. Ορίζουμε την συνάρτηση αθροίσματος*

$$U(t) = \sum_{n \leqslant t} u(n).$$

Έστω a και b μη αρνητικοί ακέραιοι με $a \leqslant b$. Τότε

$$\sum_{n=a+1}^{b} u(n)f(n) = U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)).$$

Έστω x και y πραγματικοί αριθμοί τέτοιοι ώστε $0 \leqslant y < x$. Αν $f(t)$ είναι μια συνάρτηση με συνεχή παράγωγο στο διάστημα $[x, y]$, τότε

$$\sum_{y < n \leqslant x} u(n)f(n) = U(x)f(x) - U(y)f(y) - \int_y^x U(t)f'(t)dt.$$

Ειδικότερα, αν η $f(t)$ έχει συνεχή παράγωγο στο $[1, x]$, τότε

$$\sum_{n \leqslant x} u(n)f(n) = U(x)f(x) - \int_1^x U(t)f'(t)dt.$$

Απόδειξη. Υπολογίζουμε

$$\begin{aligned}
\sum_{n=a+1}^{b} u(n)f(n) &= \sum_{n=a+1}^{b} (U(n) - U(n-1))f(n) \\
&= \sum_{n=a+1}^{b} U(n)f(n) - \sum_{n=a}^{b-1} U(n)f(n+1) \\
&= U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)).
\end{aligned}$$

Αν η συνάρτηση $f(t)$ είναι συνεχώς παραγωγίσιμη στο $[x, y]$,τότε

$$f(n+1) - f(n) = \int_n^{n+1} f'(t)dt$$

και

$$U(n)(f(n+1) - f(n)) = \int_n^{n+1} U(t)f'(t)dt.$$

Έστω $a = [y]$ και $b = [x]$. Τότε,

$$\begin{aligned}
\sum_{y<n\leqslant x} u(n)f(n) &= \sum_{n=a+1}^{b} u(n)f(n) \\
&= U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)) \\
&= U(x)f(b) - U(y)f(a+1) - \sum_{n=a+1}^{b-1} \int_n^{n+1} U(t)f'(t)dt \\
&= U(x)f(x) - U(y)f(y) - U(x)(f(x) - f(b)) - U(y)(f(a+1) - f(y)) \\
&\qquad - \int_{a+1}^{b} U(t)f'(t)dt \\
&= U(x)f(x) - U(y)f(y) - \int_y^x U(t)f'(t)dt.
\end{aligned}$$

Αν η $f(t)$ είναι συνεχώς παραγωγίσιμη στο $[1, x]$, τότε

$$\begin{aligned}
\sum_{n\leqslant x} u(n)f(n) &= u(1)f(1) + \sum_{1<n\leqslant x} u(n)f(n) \\
&= u(1)f(1) + U(x)f(x) - U(1)f(1) - \int_1^x U(t)f'(t)dt \\
&= U(x)f(x) - \int_1^x U(t)f'(t)dt
\end{aligned}$$

και η απόδειξη ολοκληρώθηκε. □

A.2 Η συνάρτηση διαιρετών

Μια αριθμητική συνάρτηση $f(n)$ λέγεται *πολλαπλασιαστική* αν

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

όποτε οι αριθμοί m, n είναι σχετικώς πρώτοι θετικοί ακέραιοι. Καθώς $f(1) = f(1 \cdot 1) = f(1)^2$ έχουμε $f(1) = 1$ ή $f(1) = 0$. Αν $f(1) = 0$ τότε $f(n) = f(n \cdot 1) = f(n)f(1) = 0$ για κάθε $n \geqslant 1$. Έτσι, αν μια αριθμητική συνάρτηση f δεν είναι η ταυτοτικά μηδενική, τότε $f(1) = 1$.

Θεώρημα A.2.1. *Έστω $f(n)$ μια πολλαπλασιαστική αριθμητική συνάρτηση. Αν*

$$\lim_{p^k\to\infty} f(p^k) = 0$$

καθώς το p^k διατρέχει την ακολουθία όλων των πρώτων αριθμών, τότε

$$\lim_{n\to\infty} f(n) = 0.$$

Απόδειξη. Υπάρχουν πεπερασμένες το πλήθος δυνάμεις πρώτων p^k τέτοιες ώστε $|f(p^k)| \geqslant 1$. Έστω

$$A = \prod_{|f(p^k)|\geqslant 1} |f(p^k)|.$$

Τότε είναι προφανές ότι $A \geqslant 1$. Έστω $0 < \varepsilon < A$. Υπάρχουν πεπερασμένες το πλήθος δυνάμεις πρώτων p^k τέτοιες ώστε $|f(p^k)| \geqslant \varepsilon/A$. Προκύπτει λοιπόν ότι υπάρχουν πεπερασμένοι ακέραιοι n τέτοιοι ώστε

$$|f(p^k)| \geqslant \varepsilon/A$$

για κάθε δύναμη πρώτου p^k που διαιρεί το n. Συνεπώς αν το n είναι αρκετά μεγάλο, ο n διαιρείται από τουλάχιστον μία δύναμη πρώτου p^k τέτοια ώστε $|f(p^k)| \leqslant \varepsilon/A$, και έτσι μπορούμε να γράψουμε τον n στην μορφή

$$n = \prod_{i=1}^{r} p_i^{k_i} \prod_{i=r+1}^{r+s} p_i^{k_i} \prod_{i=r+s+1}^{r+s+t} p_i^{k_i}$$

όπου οι $p_1, \dots, p_{r+s+t}$ είναι ανά δύο διαφορετικοί πρώτοι αριθμοί τέτοιοι ώστε

$$1 \leqslant |f(p^{k_i})|$$

για $i = 1, \dots, r$,

$$\frac{\varepsilon}{A} \leqslant |f(p^{k_i})| \leqslant 1$$

για $i = r+1, \dots, r+s$,

$$|f(p^{k_i})| \leqslant \frac{\varepsilon}{A}$$

για $i = r+s+1, \dots, r+s+t$ και $t \geqslant 1$. Έπεται από τα παραπάνω, αφού η $f(n)$ είναι πολλαπλασιαστική, ότι

$$|f(n)| = \prod_{i=1}^{r} |f(p_i^{k_i})| \prod_{i=r+1}^{r+s} |f(p_i^{k_i})| \prod_{i=r+s+1}^{r+s+t} |f(p_i^{k_i})| < A(\varepsilon/A)^t \leqslant \varepsilon$$

και η απόδειξη ολοκληρώθηκε. □

Η *συνάρτηση διαιρετών* $d(n)$ μετράει το πλήθος των θετικών διαιρετών του n. Για παράδειγμα, $d(n) = 1$ αν και μόνο αν $n = 1$, και $d(n) = 2$ αν και μόνο ο n είανι πρώτος. Επίσης είναι εύκολο να δούμε ότι είναι πολλαπλασιαστική συνάρτηση.

Θεώρημα Α.2.2. *Ισχύει*

$$d(n) \ll_\varepsilon n^\varepsilon$$

για κάθε $\varepsilon > 0$.

Απόδειξη. Θεωρούμε τη συνάρτηση $f(n) = d(n)/n$. Για να έχουμε το ζητούμενο αρκεί να δείξουμε ότι $f(n) = o(1)$. Καθώς οι αριθμητικές συναρτήσεις $d(n)$ και n είναι πολλαπλασιαστικές, προκύπτει ότι και η $f(n)$ είναι πολλαπλασιαστική. Απο το θεώρημα A.2.1 αρκεί να δείξουμε ότι

$$\lim_{p^k \to \infty} f(p^k) = 0.$$

Αφού η ποσότητα $(k+1)/2^{k\varepsilon/2}$ είναι φραγμένη για $k \geqslant 1$, έχουμε

$$f(p^k) = \frac{d(p^k)}{p^{k\varepsilon}} = \frac{k+1}{p^{k\varepsilon}} = \left(\frac{k+1}{p^{k\varepsilon/2}}\right)\left(\frac{1}{p^{k\varepsilon/2}}\right) \leqslant \left(\frac{k+1}{2^{k\varepsilon/2}}\right)\left(\frac{1}{p^{k\varepsilon/2}}\right) \ll \left(\frac{1}{p^k}\right)^{\varepsilon/2}$$

και η απόδειξη ολοκληρώθηκε. □

A.3 Άπειρα γινόμενα

Συζητάμε τέλος κάποια βασικά αποτελέσματα για τα άπειρα γινόμενα και τα γινόμενα Euler. Έστω $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$ μια ακολουθία μιγαδικών αριθμών. Το *n-οστό μερικό γινόμενο* αυτής της ακολουθίας είναι ο αριθμός

$$p_n = \alpha_1 \cdots \alpha_n = \prod_{k=1}^{n} \alpha_k$$

Αν, καθώς το n τείνει στο άπειρο, η ακολουθία των n-οστών μερικών γινομένων συγκλίνει σε ένα όριο α διαφορετικό του μηδενός, τότε λέμε ότι το άπειρο γινόμενο $\prod_{k=1}^{n} \alpha_k$ συγκλίνει και

$$\prod_{k=1}^{\infty} \alpha_k = \lim_{n\to\infty} p_n = \lim_{n\to\infty} \prod_{k=1}^{n} \alpha_k = \alpha$$

Λέμε ότι το άπειρο γινόμενο *αποκλίνει* αν το όριο της ακολουθίας των μερικών γινομένων δεν υπάρχει ή υπάρχει αλλά είναι ίσο με μηδέν. Στην τελευταία περίπτωση λέμε ότι το άπειρο γινόμενο *αποκλίνει στο μηδέν.*

Έστω

$$\alpha_k = 1 + a_k.$$

Αν το άπειρο γινόμενο $\prod_{k=1}^{\infty}(a_k+1)$ αποκλίνει, τότε $a_k \neq -1$ για όλους τους k. Επιπλέον,

$$\lim_{k\to\infty}(1+a_k) = \lim_{k\to\infty} \frac{p_k}{p_{k-1}} = 1,$$

και έτσι

$$\lim_{k\to\infty} a_k = 0.$$

Θεώρημα A.3.1. *Έστω $a_k \geqslant 0$ για όλους τους k. Το άπειρο γινόμενο $\prod_{k=1}^{\infty}(a_k+1)$ συγκλίνει αν και μόνο αν η σειρά $\sum_{k=1}^{\infty} a_k$ συγκλίνει.*

Απόδειξη. Έστω $s_n = \sum_{k=1}^{n} a_k$ το n-οστό μερικό άθροισμα και έστω $p_n = \prod_{k=1}^{n}(a_k+1)$ το n-οστό μερικό γινόμενο. Καθώς $a_n \geqslant 0$, οι ακολουθίες $\{s_n\}$ και $\{p_n\}$ είναι και οι δύο αύξουσες, και $p_n \geqslant 1$ για κάθε n. Επειδή

$$1 + x \leqslant e^x$$

για όλους τους πραγματικούς x, προκύπτει ότι

$$0 \leqslant \sum_{k=1}^{n} < \prod_{k=1}^{n}(1+a_k) \leqslant \prod_{k=1}^{n} e^{a_k} = e^{\sum_{k=1}^{n} a_k},$$

και συνεπώς

$$0 \leqslant s_n < p_n \leqslant e^{s_n}.$$

Η ανισότητα αυτή δείχνει ότι η ακολουθία $\{p_n\}$ συγκλίνει αν και μόνο αν η ακολουθία $\{s_n\}$ συγκλίνει. Αυτό ολοκληρώνει και την απόδειξη. □

Λέμε ότι το άπειρο γινόμενο $\prod_{k=1}^{\infty}(1+a_k)$ *συγκλίνει απόλυτα* αν το άπειρο γινόμενο

$$\prod_{k=1}^{\infty}(1+|a_k|)$$

συγκλίνει.

Θεώρημα Α.3.2. *Αν το άπειρο γινόμενο $\prod_{k=1}^{\infty}(1+a_k)$ συγκλίνει απόλυτα, τότε συγκλίνει.*

Απόδειξη. Έστω

$$p_n = \prod_{k=1}^{n}(1+a_k)$$

και έστω

$$P_n = \prod_{k=1}^{n}(1+|a_k|).$$

Αν το άπειρο γινόμενο συγκλίνει απόλυτα, τότε η ακολουθία των μερικών γινομένων P_n συγκλίνει και συνεπώς η σειρά

$$\sum_{n=2}^{\infty}(P_n - P_{n-1})$$

συγκλίνει. Καθώς

$$0 \leqslant |p_n - p_{n-1}| = |a_n p_{n-1}| = \left|a_n \prod_{k=1}^{n-1}(1+a_k)\right| \leqslant |a_n| \prod_{k=1}^{n-1}(1+|a_k|) = |a_n| P_{n-1} = P_n - P_{n-1},$$

προκύπτει ότι η σειρά

$$\sum_{k=2}^{\infty}|p_n - p_{n-1}|$$

συγκλίνει, και άρα η σειρά

$$\sum_{k=2}^{\infty}(p_n - p_{n-1}) = \lim_{n\to\infty}\sum_{k=2}^{n}(p_k - p_{k-1}) = \lim_{n\to\infty}(p_n - p_1)$$

συγκλίνει. Έτσι, η ακολουθία των μερικών γινομένων $\{p_n\}$ συγκλίνει σε κάποιο πεπερασμένο όριο.

Πρέπει να αποδείξουμε ότι το όριο αυτό είναι διάφορο του μηδενός. Αφού το άπειρο γινόμενο $\prod_{k=1}^{\infty}(1+a_k)$ συγκλίνει απόλυτα, έπεται από το προηγούμενο θεώρημα ότι η σειρά $\sum_{k=1}^{\infty}|a_k|$ συγκλίνει, και έτσι η ακολουθία a_k συγκλίνει στο 0. Συνεπώς, για όλους τους αρκετά μεγάλους k,

$$|1+a_k| \geqslant 1/2$$

και

$$\left|\frac{-a_k}{1+a_k}\right| \leqslant 2|a_k|.$$

Προκύπτει με αυτόν τον τρόπο ότι η σειρά

$$\sum_{k=1}^{\infty}\left|\frac{-a_k}{1+a_k}\right|$$

συγκλίνει και άρα το άπειρο γινόμενο

$$\prod_{k=1}^{\infty}\left(1-\frac{a_k}{1+a_k}\right)$$

συγκλίνει απόλυτα. Από αυτό έπεται ότι η ακολουθία των n-οστών μερικών γινομένων

$$\prod_{k=1}^{n}\left(1-\frac{a_k}{1+a_k}\right) = \prod_{k=1}^{n}\frac{1}{1+a_k} = \frac{1}{\prod_{k=1}^{n}(1+a_k)} = \frac{1}{p_n}$$

συγκλίνει σε ένα πεπερασμένο όριο και άρα το όριο της ακολουθίας $\{p_n\}$ είναι μη μηδενικό. Συμπεραίνουμε λοιπόν ότι το άπειρο γινόμενο $\prod_{k=1}^{\infty}(1+a_k)$ συγκλίνει. □

Ένα *γινόμενο Euler* είναι ένα άπειρο γινόμενο που εκτείνεται στους πρώτους αριθμούς. Συμβολίζουμε τα αθροίσματα και τα γινόμενα πάνω στους πρώτους με $\sum_p$ και $\prod_p$, αντίστοιχα.

Θεώρημα Α.3.3. *Έστω $f(n)$ μια πολλαπλασιαστική συνάρτηση που δεν είναι η ταυτοτικά μηδενική. Αν η σειρά*

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

συγκλίνει απόλυτα, τότε

$$\sum_{n=1}^{\infty} f(n) = \prod_p \left(1+f(p)+f(p^2)+\cdots\right) = \prod_p \left(1+\sum_{k=1}^{\infty} f(p^k)\right).$$

Αν η $f(n)$ είναι πλήρως πολλαπλασιαστική, τότε

$$\sum_{n=1}^{\infty} f(n) = \prod_p \left(1-f(p)\right)^{-1}.$$

Απόδειξη. Αν η $\sum_{n=1}^{\infty} f(n)$ συγκλίνει απόλυτα, τότε η σειρά

$$a_p = \sum_{k=1}^{\infty} f(p^k)$$

συγκλίνει απόλυτα για κάθε πρώτο p. Επίσης η σειρά

$$\sum_p |a_p| = \sum_p \left| \sum_{k=1}^{\infty} f(p^k) \right| \leqslant \sum_p \sum_{k=1}^{\infty} |f(p^k)| < \sum_{n=1}^{\infty} |f(n)|$$

συγκλίνει, και έτσι προκύπτει ότι το άπειρο γινόμενο

$$\prod_p (1 + a_p) = \prod_p \left(1 + \sum_{k=1}^{\infty} f(p^k) \right)$$

συγκλίνει απόλυτα. Από το Θεώρημα Α.3.2 προκύπτει ότι συγκλίνει.

Έστω $\varepsilon > 0$. Διαλέγουμε ακέραιο N_0 τέτοιον ώστε

$$\sum_{n > N_0} |f(n)| < \varepsilon.$$

Για κάθε θετικό ακέραιο n, έστω $P(n)$ ο μέγαλύτερος πρώτος παράγοντας του n. Τότε με $\sum_{P(n) \geqslant N}$ συμβολίζουμε το άθροισμα πάνω από όλους τους ακεραίους οι οποίοι έχουν τουλάχιστον έναν πρώτο παράγοντα γνήσια μεγαλύτερο του N. Αφού η σειρά $\sum_{k=0}^{\infty} f(p^k)$ συγκλίνει απόλυτα για κάθε πρώτο αριθμό p, μπορούμε να πολλαπλασιάσουμε κάθε πεπερασμένο πλήθος αυτών των σειρών όρο προς όρο. Έστω $N \geqslant N_0$. Από τη μοναδικότητα της παραγοντοποίησης των ακεραίων σε γινόμενο πρώτων προκύπτει ότι

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

άρα

$$\begin{aligned} \left| \sum_{n=1}^{\infty} f(n) - \prod_{p \leqslant N} \left(1 + \sum_{k=1}^{\infty} f(p^k) \right) \right| &= \left| \sum_{n=1}^{\infty} f(n) - \sum_{P(n) \geqslant N} f(n) \right| \\ &= \left| \sum_{P(n) > N} f(n) \right| \\ &\leqslant \sum_{P(n) > N} |f(n)| \leqslant \sum_{n > N} |f(n)| \leqslant \sum_{n > N_0} |f(n)| < \varepsilon. \end{aligned}$$

Έπεται ότι

$$\sum_{n=1}^{\infty} f(n) = \lim_{N \to \infty} \prod_{p \leqslant N} \left(1 + \sum_{k=1}^{\infty} f(p^k) \right) = \prod_p \left(1 + \sum_{k=1}^{\infty} f(p^k) \right).$$

Αν η $f(n)$ είναι πλήρως πολλαπλασιαστική, τότε $f(p^k) = f(p)^k$ για όλους τους πρώτους p και όλους τους μη αρνητικούς ακεραίους k. Εφόσον το $f(p^k)$ τείνει στο άπειρο όταν το k τείνει στο άπειρο, έχουμε ότι $|f(p)| < 1$. Αθροίζοντας την γεωμετρική πρόοδο έχουμε

$$\left(1 + \sum_{k=1}^{\infty} f(p^k) \right) = \left(1 + \sum_{k=1}^{\infty} f(p)^k \right) = \frac{1}{1 - f(p)},$$

συνεπώς

$$\prod_p \left(1 + \sum_{k=1}^{\infty} f(p^k) \right) = \prod_p (1 - f(p))^{-1}$$

και η απόδειξη είναι πλήρης. □

Βιβλιογραφία

[1] N. N. Bogolyubov, *Sur quelques propriétés arithmétiques des presques-périodes*, Ann. Chaire Math. Phys. Liev **4** (1939), 185–194.

[2] J. W. S. Cassels, *An introduction to the Geometry of Numbers*, Springer-Verlag, Berlin, 1959.

[3] A. Y. Khinchin, *Three pearls of number theory*, Dover Publications, Inc., Mineola, NY, 1998.

[4] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics, 165. Springer-Verlag, New York, 1996.

[5] M. B. Nathanson, *Additive number theory. The classical bases*, Graduate Texts in Mathematics, 164. Springer-Verlag, New York, 1996.

[6] L. G. Shnirel'man, *Über additive Eigenschaften von Zahlen*, Math. Annalen **107** (1933), 649–690.

[7] C. L. Siegel, *Lectures on the Geometry of Numbers*, Springer-Verlag, Berlin, 1989.

[8] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245.

[9] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006.

[10] E. Wirsing, *Ein metrischer Satz über Mengen ganzer Zahlen*, Arxhiv Math. **4** (1953), 392–398.