Προσθετική θεωρία αριθμών

Διπλωματική Εργασία

Αλέξανδρος Ηλιόπουλος

Τμήμα Μαθηματικών
Πανεπιστήμιο Αθηνών
Αθήνα – 2019

Μέρος I

Το πρόβλημα του **Waring**

ΚΕΦΑΛΑΙΟ 1

Το θεώρημα Hilbert-Waring

1.1 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 1.1.1 (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

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

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

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

είναι το άθροισμα 12 τέταρτων δυνάμεων. Κάθε μη αρνητικός ακέραιος n μπορεί να γραφεί στην μορφή $n = 6q+r$, με $q \geq 0$ και $0 \leqslant r \leqslant 5$. Από το θεώρημα του Lagrange προκύπτει ότι $q = a_1^2+...+a_4^2$ και συνεπώς $6q = 6a_1^2+...6a_4^2$ 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 1.1.2 (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 1.1.3 (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 έκτων δυνάμεων.

Ας υποθέσουμε ότι

$$(x_1^2+x_2^2+x_3^2+x_4^2)^k = \sum_{i=1}^{M}a_i(b_{i,1}x_1^2+b_{i,2}x_2^2+b_{i,3}x_3^2+b_{i,4}x_4^2)^{2k} \tag{1.1.1}$$

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 (1.1.1) 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.

1.2 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

$$H_{n+1}(x) = xH_n(x) - \frac{1}{2}H_n'(x). \tag{1.2.1}$$

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 1.2.1. *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 $H_1(x) = x$. Έστω $n \geq 1$, και υποθέτουμε ότι το λήμμα ισχύει για 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 το για το H_{n+1} ως 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 το n ειναι περιττος. Σε κάθε λοιπον περίπτωση το $H_{n+1}(x)$ έχει $n+1$ το πλήθος και διαφορετικές μεταξύ τους πραγματικές ρίζες. □

Λήμμα 1.2.2. *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 1.2.3. *Για κάθε άρτιο $n \geqslant 0$ ισχύει*

$$c_n = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} x^n \, dx = \frac{n!}{2^n (n/2)!}, \tag{1.2.2}$$

ενώ αν ο $n \geqslant 0$ 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 $n-2$. Ολοκληρώνοντας κατά μέρη παίρνουμε

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

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 1.2.4. *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* (1.2.2) *τότε το σύστημα γραμμικών εξισώσεων*

$$\sum_{j=1}^{n} \beta_j^k x_j = c_k, \qquad k = 0, 1, \ldots, n-1 \tag{1.2.3}$$

έχει μοναδική λύση $\varrho_1, \ldots, \varrho_n$. Για κάθε πολυώνυμο 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

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

είναι η ορίζουσα Vandermode

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

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

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

□

Λήμμα 1.2.5. *Έστω $n \geqslant 1$ και $\beta_1, \dots, \beta_n$ οι n διακεκριμένες πραγματικές ρίζες του n-οστού πολυωνύμου Hermite $H_n(x)$. Αν $\varrho_1, \dots, \varrho_n$ είναι η λύση του συστήματος γραμμικών εξισώσεων (;;) 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 $j = 1, \dots, n$, έχουμε

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

Από το Λήμμα 1.2.4 και το Λήμμα 1.2.2,

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

και έχουμε το ζητούμενο. □

Λήμμα 1.2.6. *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 (;;) 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 $2n - 2$ και τέτοιο ώστε $f_i(x) \geq 0$ 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 1.2.5 παίρνουμε ότι

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

και έτσι έχουμε το ζητούμενο. □

Λήμμα 1.2.7. *Έστω $n \geqslant 1$ και $c_0, c_1, \ldots, c_{n-1}$ οι ρητοί αριθμοί που ορίζονται από την (;;). 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 1.2.4, για κάθε n-αδα διαφορετικών ανά δύο πραγματικών αριθμών $\beta_1, \beta_2, \ldots, \beta_n$ το σύστημα των n γραμμικων εξισώσεων στους 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 $(\beta_1, \beta_2, \ldots, \beta_n)$ τέτοια ώστε $\beta_i \neq \beta_j$ 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 1.2.6, αν οι $\beta_1, \beta_2, \ldots, \beta_n$ 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 στο $\Re$. Έτσι τα σημεία με ρητές συντεταγμένες έιναι πυκνά στο $\Re$ και συνεπώς 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 1.2.8. *Έστω $n \geqslant 1$ και $c_0, c_1, \ldots, c_{n-1}$ οι ρητοί αριθμοί που ορίζονται από την* (;;). *Έστω επίσης $\beta_1, \ldots, \beta_n$ διακεκριμένοι πραγματικοί αριθμοί, και $\varrho_1, \ldots, \varrho_n$ η λύση του γραμμικού συστήματος* (;;). *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

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

Από το Λήμμα 1.2.3 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 (;;), παίρνουμε

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

το οποίο ολοκληρώνει την απόδειξη. □

Θεώρημα 1.2.9 (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_{ij}, για $i=1,\dots,M$ και $j=1,\dots,r$, τέτοιους ώστε*

$$(x_1^2+\cdots+x_r^2)^k=\sum_{i=1}^{M}(b_{i1}x_1+\cdots+b_{ir}x_r)^{2k}.$$

Απόδειξη. Επιλέγουμε $n>2k$ και θεωρούμε τους ρητούς αριθμούς $\beta_1^*,\dots,\beta_n^*,\varrho_1^*,\dots,\varrho_n^*$ που κατασκευάστηκαν στο Λήμμα 1.2.7. Οι $\beta_1^*,\dots,\beta_n^*$ είναι διακεκριμένοι και οι $\varrho_1^*,\dots,\varrho_n^*$ είναι θετικοί. Χρησιμοποιώντας αυτούς τους αριθμούς στο Λήμμα **;;** 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 1.2.10. *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*

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

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 (;;). Έστω q ο ελάχιστος κοινός παρονομαστής 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

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

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

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

Το Λήμμα 1.2.10 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 1.2.11. *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 (;;) για τον k με $r = 4$:

$$(x_1^2 + \cdots + x_4^2)^k = \sum_{i=1}^{M} a_i (b_{i1}x_1 + \cdots + b_{i4}x_4)^{2k}.$$

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

$$y^k = \sum_{i=1}^{M} a_i z_i^{2k}, \tag{1.2.4}$$

όπου οι

$$z_i = b_{i1}x_1 + \cdots + b_{i4}x_4$$

είναι μη αρνητικοί ακέραιοι. Αυτό σημαίνει ότι

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

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 1.2.10, το πρόβλημα του Waring έχει θετική απάντηση και για τον εκθέτη $2k$. □

1.3 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 1.3.1. *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, τέτοιο ώστε*

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

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

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

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 στα αριστερά της σχέσης $(;;)$ 2ℓ φορές παίρνουμε

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

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

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

όπου $y_i = |b_ix+c_i|$ 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 $U \geq 0$, 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

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

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

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

καταλήγουμε ότι

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

$$=\frac{\sum_{i=1}^{M_\ell}a_i'y_i^{2k}}{A_{\ell,\ell}^{k-\ell+1}}=\sum_{i=1}^{M_\ell}a_i''y_i^{2k}=\sum(2k)$$

και η απόδειξη του λήμματος ολοκληρώθηκε. □

Θεώρημα 1.3.2 (Hilbert-Waring)**.** *Το σύνολο των μη αρνητικών k-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 **;;** του Lagrange. Έστω λοιπόν $k\geq 3$, και υποθέτουμε ότι το σύνολο των ℓ-δυνάμεων έιναι βάση πεπερασμένης τάξης για κάθε $\ell<k$. Από το Θεώρημα **;;**, το σύνολο των 2ℓ-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 $T\geq 2$. Διαλέγουμε 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

$$x_{1,\ell}^{2\ell}+\cdots+x_{r,\ell}^{2\ell}=C_{k-\ell}. \tag{1.3.1}$$

Τότε

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

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

$$x_{j,\ell}^{2\ell}T^{k-\ell}+\sum_{i=0}^{\ell-1}B_{i,\ell}x_{j,\ell}^{2i}T^{k-i}=\sum(2k)=\sum(k) \tag{1.3.2}$$

Αθροίζοντας την (1.3.2) για $j = 1, \dots, r$ και χρησιμοποιώντας την (1.3.1), 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 $\ell = 1, \dots, k-1$. Ο ακέραιος $D_{k-\ell+1}$ καθορίζεται πλήρως από τους k, ℓ, T και $C_{k-\ell}$ και είναι ανεξάρτητος του C_{k-i} για $i \neq \ell$. Έστω

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

Έπεται ότι

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

όπου χρησιμοποιήθηκαν τα εξής:

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

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

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

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

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

καθορίζεται από τον k και είναι ανεξάρτητος του T. Αν διαλέξουμε

$$T\geq E^*,$$

έπεται

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

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

$$\sum_{\ell=1}^{k}(C_\ell+D_\ell)T^\ell=E_1T+\cdots+E_{k-1}T^{k-1}+E_kT^k, \tag{1.3.3}$$

με

$$0\leqslant E_i<T$$

για $i=1,\ldots,k-1$ και

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

Με αυτόν τον τρόπο, δείξαμε ότι για κάθε επιλογή μιας $(k-1)$-άδας $(C_1,\ldots,C_{k-1})$ ακεραίων ανάμεσα στους $\{0,1,\ldots,T-1\}$ καθορίζει μια άλλη $(k-1)$-άδα $(E_1,\ldots,E_{k-1})$ ακεραίων ανάμεσα στους $\{0,1,\ldots,T-1\}$. 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 ανάμεσα στους $\{0,1,\ldots,T-1\}$. Υπάρχει ένας απλός αλγόριθμος που παράγει ακεραίους $C_1,C_2,\ldots,C_{k-1}\in\{0,1,\ldots,T-1\}$ τέτοιους ώστε η (1.3.3) ικανοποιείται για κάποιον μη αρνητικό ακέραιο $E_k<E^*$. Έστω $C_1=E_1$ και $I_2=0$. Καθώς $D_1=0$, έχουμε

$$(C_1+D_1)T=E_1T+I_2T^2.$$

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

$$C_2+D_2+I_2\equiv E_2(modT).$$

Συνεπώς

$$C_2+D_2+I_2=E_2+I_3T$$

για κάποιον ακέραιο I_3, και

$$\sum_{\ell=1}^{2}(C_\ell+D_\ell)T^\ell=\sum_{\ell=1}^{2}E_\ell T^\ell+I_3T^3.$$

Ακριβώς με τον ίδιο τρόπο ο ακέραιος C_2 καθορίζει τον D_3. Όμοια διαλέγουμε $C_3 \in \{0, 1, \ldots, T-1\}$ τέτοιον ώστε

$$C_3 + D_3 + I_3 \equiv E_3 (mod T)$$

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

$$C_j + D_j + I_j \equiv E_j (mod T)$$

Έτσι

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

για κάποιον ακέραιο I_{j+1}, και

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

Επαγωγικά, 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} καθορίζει 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

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

και

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

προκύπτει ότι

$$\sum_{\ell=1}^{k-1} E_\ell T^\ell + E^* T^k < (1+E^*)T^k \leqslant 2E^* T^k. \tag{1.3.4}$$

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

$$\sum_{\ell=1}^{k-1} E_\ell T^\ell + E^* T^k = \sum(k) \tag{1.3.5}$$

για κάθε $(k-1)$-άδα ακεραίων $(E_1, \ldots, E_{k-1})$ ανάμεσα στους $\{0, 1, \ldots, T-1\}$. Καθώς η $\left(\frac{T+1}{T}\right)^k$ συγκλίνει στο 1 καθώς T τείνει στο άπειρο μπορούμε να διαλέξουμε ακέραιο $T_0 > 5E^*$ με

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

για κάθε $T \geq T_0$. Θα δείξουμε ότι εάν $T \geq T_0$ 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 (1.3.4) με $T+1$ στη θέση του T, παίρνουμε

$$E_0'(T+1) + E^*(T+1)^k < (T+1)^2 + E^*(T+1)^k \leqslant (1+E^*)(T+1)^k \leqslant 2E^*(T+1)^k. \tag{1.3.6}$$

Ακόμα, εφαρμόζοντας την (1.3.5) με $T+1$ στην θέση του T , έχουμε

$$E_0'(T+1) + E^*(T+1)^k = \sum(k) \tag{1.3.7}$$

Προσθέτοντας τώρα τις (1.3.5) και (1.3.7), βλέπουμε ότι για κάθε επιλογή k το πλήθος ακεραίων

$$E_0', E_1, \ldots, E_{k-1} \in \{0, 1, \ldots, T-1\},$$

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 (1.3.4) και (1.3.6) 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 $T \geq T_0 > 5E^*$. Δοθέντων k ακεραίων μπορούμε να εφαρμόσουμε πάλι τον αλγόριθμο για να βρούμε ακεραίους F_k και

$$E_0', , E_1, \ldots, E_{k-1} \in \{0, 1, \ldots, T-1\},$$

τέτοιους ώστε

$$\begin{aligned} &F_0 + F_1T + \cdots + F_{k-1}T^{k-1} + F_kT^k \\ &= E_1T + \cdots + E_{k-1}T^{k-1} + E^*T^k + E_0'(T+1) + E^*(T+1)^k \\ &= \sum(k), \end{aligned}$$

όπου ο F_k είναι ένας ακέραιος που ικανοποιεί την ανισότητα

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

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

$$F_0 + F_1T + \cdots + F_{k-1}T^{k-1} + 5E^*T^k = \sum(k)$$

για όλα τα $T \geq T_0$ 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 $T \geq T_0$ και

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

Υπάρχει ένας ακέραιος $T_1 \geq T_0$ με

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

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

$$5E^*T^k \leqslant n < 5E^*(T+1)^k. \tag{1.3.8}$$

Καθώς κάθε ακέραιος $n \geq 5E^*T_1^k$ ικανοποιεί την ανισότητα (1.3.8) για κάποιον $T \geq T_1$, συμπεραίνουμε ότι

$$n = \sum(k)$$

για όλα τα n με $n \geq 5E^*T_1^k$. Το τελικό συμπέρασμα τώρα προκύπτει άμεσα από το λήμμα 3.9. □

ΚΕΦΑΛΑΙΟ 2

Η ανισότητα του Weyl

2.1 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 έπίσης 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 $\lfloor x \rfloor$ το ακέραιο μέρος του πραγματικού αριθμού x και με $\{x\}$ το κλασματικό μέρος του x, δηλαδή $\{x\} = x - \lfloor x \rfloor$.

Θεώρημα 2.1.1 (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 κάποιο 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 κάποιο θετικό ακέραιο αριθμό $q \leqslant N$ και αν $a = [q\alpha]+1$,τότε καθώς

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

έυκολα 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

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

και 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. □

2.2 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 2.2.1. *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 ℓ, τότε έχουμε

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

όπου στην τελευταία ισότητα χρησιμοποιήθηκε η γνωστη 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 2.2.2. *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

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

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

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

όπου στην 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 $\frac{k!}{(k-\ell)!} = k(k-1)\cdots(k-\ell+1)$ ο.ε.δ. □

Λήμμα 2.2.3. *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 2.2.2 έχουμε

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

Για να ισχύει η σχέση $j_1 + \cdots + j_{k-1} + j = k$ με $j_1, \ldots, j_{k-1} \geq 1$ και $j \geq 0$ 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 2.2.4. *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 $f(x) = \sum_{j=1}^k x^j$, 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 2.2.5. *Έστ$1 \leqslant \ell \leqslant k$. 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 2.2.2 και καθώς $-P \leqslant d_1, \ldots, d_\ell, x \leqslant P$ εύκολα προκύπτει ότι

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

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

$$n = \pm x_1^k \pm x_2^k \pm \cdots \pm x_{v(k)}^k \tag{2.2.1}$$

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 2.2.6 (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 2.2.1 και 2.2.3 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 είναι εύκολο να δούμε ότι για κάθε ακέραιο n μπορούμε να βρούμε ακέραιους 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 $\pm x^k$. □

2.3 Κλασματικά μέρη

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

$$\alpha = \lfloor \alpha \rfloor + \{\alpha\}.$$

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 ότι

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

για κάθε πραγματικό αριθμό α. Η τριγωνική ανισότητα

$$\|\alpha+\beta\| \leqslant \|\alpha\| + \|\beta\| \tag{2.3.1}$$

ισχύει για κάθε ζεύγος πραγματικών αριθμών α και β.

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 2.3.1. *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 2.3.2. *Για κάθε πραγματικό αριθμό α και για οποιουσδήποτε φυσικούς $N_1 < N_2$,*

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

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

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

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 2.3.3. *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 $q \geq 2$. 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

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

Καθώς $(a,q)=1$ έχουμε

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

και έτσι $s(r) \in [1, q/2]$ αν και μόνο αν $r \in [1,/2]$. 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

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

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

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

όπου στην πρώτη ανισότητα χρησιμοποιήσαμε την τριγωνική ανισότητα. Στην 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

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

$$\Leftrightarrow ar_1 \equiv \pm ar_2 (mod q) \Leftrightarrow r_1 \equiv \pm r_2 (mod q).$$

όπου στην τελευταία ισοδυναμία χρησιμοποιήσαμε το ότι οι a και q είναι σχετικά πρώτοι μεταξύ τους αριθμοί. Αν $r_1 = r_2 (mod q)$ τότε καθώς $1 \leqslant r_1 \leqslant r_2 \leqslant q/2$ είναι φανερό ότι $r_1 = r_2$. Αν τώρα $r_1 = -r_2 (mod q)$ 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

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

και έτσι,

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

και η απόδειξη ολοκληρώθηκε. □

Λήμμα 2.3.4. *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 ένας 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

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

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 ακεραίους. Αν $1 \leqslant r_1 \leqslant r_2 \leqslant q$ και

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

τότε

$$ar_1 \equiv ar_2 (mod q)$$

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

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

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

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

Συγκεκριμένα, αν θεωρήσουμε $J(s) = [s/q, (s+1)/q]$ 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 $s \geq 1$,χρησιμοποιούμε την ανισότητα

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

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 και την απόδειξη του λήμματος. □

Λήμμα 2.3.5. *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 πραγματικό αριθμό $U \geqslant 1$ και κάθε φυσικό n, έχουμε

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

Απόδειξη. Μπορούμε να γράψουμε τον k στην μορφή

$$k = hq + r,$$

όπου

$$1 \leqslant r \leqslant q$$

και

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

Τότε

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

Αν $h=0$ και $1 \leqslant r \leqslant q/2$, τότε από το λήμμα 2.3.3 προκύπτει

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

Για τους υπόλοιπους όρους, έχουμε

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

καθώς είτε $h \geq 1$ και

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

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

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

Έτσι,

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

Παρατηρούμε ότι

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

Υπολογίζοντας τώρα το εσωτερικό άθροισμα από το λήμμα 2.3.4 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 2.3.6. *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 οποιουσδήποτε 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 2.3.5. Έχουμε

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

Αυτό ολοκληρώνει την απόδειξη. □

2.4 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 $e(t) = e^{2\pi it}$ είναι ο $\overline{e(t)} = e(-t)$.

Λήμμα 2.4.1. *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

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

Αυτός είναι ο ισχυρισμός του λήμματος. □

Λήμμα 2.4.2. *Έστω N_1, N_2, N και ℓ ακέραιοι τέτοιοι ώστε $\ell \geqslant 1, N, N_1, N_2$ 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,

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

όπου

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

και $I(d_\ell, \dots, d_1)$ 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 2.4.1. Υποθέτουμε ότι το αποτέλεσμα ισχύει για κάποιον $\ell \geqslant 1$. Χρησιμοποιώντας την ανισότητα Cauchy-Schwarz παίρνουμε

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

όπου $S_{d_\ell,\dots,d_1}(f)$ είναι ένα εκθετικό άθροισμα της μορφής (**;;**). Από το Λήμμα 2.4.1, για κάθε $d_1, \dots, d_\ell$ υπάρχει κάποιο διάστημα

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

τέτοιο ώστε

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

άρα

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

Αυτό ολοκληρώνει την απόδειξη. □

Λήμμα 2.4.3. *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 2.4.2 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

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

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

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

Από το Λήμμα 2.2.4, για οποιουσδήποτε μη μηδενικούς ακεραίους $d_1,\ldots,d_{k-1}$, ο τελεστής διαφορών $\Delta_{d_{k-1},\ldots,d_1}$ εφαρμοσμένος στο πολυώνυμο $f(x)$ βαθμού k μας δίνει το γραμμικό πολυώνυμο

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

όπου

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

και $\beta \in \mathbb{R}$. Έστω $I(d_{k-1},\ldots,d_1) = [N_1+1, N_2]$. Από το Λήμμα 2.3.2,

$$\begin{aligned}
|S_{d_{k1},\ldots,d_1}(f)| &= \Big| \sum_{n\in I(d_{k-1},\ldots,d_1)} e(\Delta_{d_{k-1},d_{k-2},\ldots,d_1}(f)(n)) \Big| \\
&= \Big| \sum_{n=N_1+1}^{N_2} e(\lambda n + \beta) \Big| \\
&= \Big| \sum_{n=N_1+1}^{N_2} e(\lambda n) \Big| \\
&\ll \frac{1}{\|\lambda\|} \\
&= \frac{1}{\|d_{k-1}\cdots d_1 k!\alpha\|}.
\end{aligned}$$

Έπεται ότι

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

Συνεπώς,

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

Αφού 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, έπεται ότι

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

με την 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 $\tau(m)$ ικανοποιεί την $\tau(m) \ll_\varepsilon m^\varepsilon$ 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 την σταθερά στην ανισότητα να εξαρτάται από τα k και ε. Έτσι, ολοκληρώνεται η απόδειξη. □

Θεώρημα 2.4.4 (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*

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

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.

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 2.4.3 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 2.3.6 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 2.4.5. *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 2.4.6. *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 2.4.7 (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 2.2.2 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 2.4.2 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

$$|T(\alpha)|^{2^j} \leqslant N^{2^j-j+1} \sum_{d} r(d) e(\alpha d), \tag{2.4.1}$$

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 2.2.5, έχουμε

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

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,

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

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

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

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 (2.4.1) έπεται ότι

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

και έχουμε αποδείξει το θεώρημα. □

ΚΕΦΑΛΑΙΟ 3

Ο ασυμπτωτικός τύπος των Hardy-Littlewood

3.1 Η μέθοδος του κύκλου

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

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

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

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

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

$$r_{k,s}(N) = \mathcal{G}(N)\Gamma\Big(1+\frac{1}{k}\Big)^s \Gamma\Big(\frac{s}{k}\Big)^{-1} N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\delta}), \tag{3.1.1}$$

όπου $\Gamma(x)$ είναι η συνάρτηση Γάμμα και $\mathcal{G}(N)$ είναι η λεγόμενη «ιδιάζουσα σειρά», μια αριθμητική συνάρτηση που είναι ομοιόμορφα φραγμένη, από πάνω και από κάτω, από θετικές σταθερές που εξαρτώνται μόνο από τους k και s. Θα αποδείξουμε ότι ο ασυμπτωτικός τύπος (3.1.1) ισχύει για τον $s_0(k) = 2^k + 1$.

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

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

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

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

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

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

με

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

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

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

για κάθε $\varrho \in (0,1)$.

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

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

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

Τότε,

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

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

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

τότε παίρνουμε το τριγωνομετρικό πολυώνυμο

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

και

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

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

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

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

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

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

Τότε,

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

και

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

3.2 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 3.2.1. *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. □

3.3 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 $rk, s(N)$ για κάθε $k \geqslant 2$ και $s \geqslant s_0(k)$. Σε αυτό το κεφάλαιο αποδεικνύουμε τον ασυμπτωτικό τύπο των Hardy-Littlewood για $s \geqslant 2^k + 1$. Για $N \geqslant 2^k$ θέτουμε

$$P = \lfloor N^{1/k} \rfloor \tag{3.3.1}$$

και

$$F(\alpha) = \sum_{m=1}^{P} e(\alpha m^k). \tag{3.3.2}$$

Το τριγωνομετρικό πολυώνF(α) 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

$$r_{k,s}(N) = \int_0^1 F(\alpha)^s e(-N\alpha)\, d\alpha. \tag{3.3.3}$$

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

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

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

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

Για

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

θέτουμε

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

και

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

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

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

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

και

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

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

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

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

που δεν μπορεί να ισχύει για $P \geqslant 2$ και $k \geqslant 2$. Συνεπώς, τα μείζονα τόξα $\mathcal{M}(q,a)$ είναι ξένα ανά δύο.

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

$$\mu(\mathcal{M}) = \frac{2}{P^{k-\nu}} \sum_{1 \leqslant q \leqslant P^\nu} \varphi(q) \leqslant \frac{2}{P^{k-\nu}} \sum_{1 \leqslant q \leqslant P^\nu} q \leqslant \frac{2}{P^{k-\nu}} \frac{P^\nu(P^\nu+1)}{2} \leqslant \frac{2}{P^{k-3\nu}}, \tag{3.3.4}$$

που τείνει στο 0 όταν το P τείνει στο άπειρο.

Το σύνολο

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

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

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

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

3.4 Τα ελάσσονα τόξα

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

Θεώρημα 3.4.1. *Έστω $k \geqslant 2$ και $s \geqslant 2^k + 1$. Υπάρχει $\delta_1 > 0$ τέτοιος ώστε*

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

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

Απόδειξη. Εφαρμόζοντας το Θεώρημα 2.1.1 (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

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

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

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

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

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

συμπεραίνουμε ότι

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

το οποίο είναι άτοπο. Συνεπώς,

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

Θέτουμε

$$K = 2^{k-1}. \tag{3.4.1}$$

Από την ανισότητα του Weyl (Θεώρημα 2.4.4) 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 2.4.7) παίρνουμε

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

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. □

3.5 Τα μείζονα τόξα

Ορίζουμε τις βοηθητικές συναρτήσεις

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

και

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

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

Η ανισότητα $|S(q,a)| \leqslant q$ είναι απλή. Από την ανισότητα του Weyl (θεώρημα 2.4.5) έχουμε

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

άρα

$$\frac{S(q,a)}{q} \ll q^{-\frac{1}{K}+\varepsilon}, \tag{3.5.1}$$

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

Λήμμα 3.5.1. *Αν $|\beta| \leqslant 1/2$, τότε*

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

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

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

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

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

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

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

Ορίζουμε $U(t) = \sum_{m \leqslant t} e(\beta m)$. Από το Λήμμα 2.3.2 έχουμε $U(t) \ll \|\beta\|^{-1} = |\beta|^{-1}$. Αθροίζοντας κατά μέρη (Θεώρημα **;;**) βλέπουμε ότι

$$\begin{aligned}\sum_{m=M+1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) &= f(N)U(N) - f(M)U(M) - \int_M^N U(t) f'(t)\, dt \\ &\ll \frac{1}{|\beta|} M^{\frac{1}{k}-1} \leqslant |\beta|^{-\frac{1}{k}} \ll \min\{P, |\beta|^{-\frac{1}{k}}\}.\end{aligned}$$

Συνεπώς,

$$\begin{aligned}v(\beta) &= \sum_{m=1}^{M} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) + \sum_{m=M+1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \\ &\ll \min\{P, |\beta|^{-\frac{1}{k}}\}.\end{aligned}$$

Αυτό αποδεικνύει το λήμμα. □

Λήμμα 3.5.2. *Έστω q και α ακέραιοι τέτοιοι ώστε $1 \leqslant q \leqslant P^\nu$, $0 \leqslant \alpha \leqslant q$, και $(a, q) = 1$. Αν $\alpha \in \mathcal{M}(q, a)$, τότε*

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

Απόδειξη. Θέτουμε $\beta = \alpha - a/q$. Τότε $|\beta| \leqslant P^{\nu-k}$ 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. Έστω $y \geqslant 1$. Αφού $|S(q,a)| \leqslant q$, έχουμε

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

Έστω $t \geqslant 1$. Αφού $v(\beta) \ll P$, 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 3.5.3. *Έστω*

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

και

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

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

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

όπου $\delta_2 = (1-5\nu)/k > 0$.

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

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

Θέτουμε

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

Αφού $|S(q,a)| \leqslant q$, έχουμε $|V| \ll |v(\beta)| \ll P$ από το Λήμμα 3.5.1. Θέτουμε $F = F(\alpha)$. Τότε, $|F| \leqslant P$. Αφού $F - V = O(P^{2\nu})$ από το Λήμμα 3.5.2, έπεται ότι

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

Αφού $\mu(\mathcal{M}) \ll P^{3\nu-k}$ από την (3.3.4), έπεται ότι

$$\int_{\mathcal{M}} |F^s - V^s|\, d\alpha \ll P^{3\nu-k}P^{s-1+2\nu} = P^{s-k-\delta_2},$$

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

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

Για $q \geqslant 2$ έχουμε

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

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

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

Συνεπώς,

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

και έχουμε το θεώρημα. □

3.6 Το ιδιάζον ολοκλήρωμα

Στη συνέχεια θεωρούμε το ολοκλήρωμα

$$J(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta N)\, d\beta. \tag{3.6.1}$$

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

Θεώρημα 3.6.1. *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. Από το Λήμμα 3.5.1 έχουμε

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

και

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

όπου $\delta_3 = \nu(s/k-1) > 0$. □

Λήμμα 3.6.2. *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

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

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

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

Συνεπώς,

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

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

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

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

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

και

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

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

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

και

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

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 3.6.3. *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 3.6.2 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 3.6.2 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

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

Άρα,

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

και έχουμε ολοκληρώσει το επαγωγικό βήμα. □

3.7 Η ιδιάζουσα σειρά και το θεώρημα των Hardy και Littlewood

Στο Θεώρημα 3.5.3 ορίσαμε την συνάρτηση

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

όπου

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

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

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

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

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

όπου

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

Από την (3.5.1) βλέπουμε ότι

$$A_N(q) \ll \frac{q}{q^{\frac{s}{K}-s\varepsilon}} \leqslant \frac{1}{q^{1+\delta_4}}, \tag{3.7.1}$$

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

$$|\mathcal{G}(N)| < c_2 \tag{3.7.2}$$

για όλους τους φυσικούς N. Επιπλέον,

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

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

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

για όλους τους φυσικούς N. Αρχίζουμε δείχνοντας ότι η $A_N(q)$ είναι πολλαπλασιαστική συνάρτηση του q.

Λήμμα 3.7.1. *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 3.7.2. *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 3.7.1 προκύπτει ότι

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

και έχουμε το ζητούμενο. □

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

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

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

Λήμμα 3.7.3. *Έστω $s\geqslant 2^k+1$. Για κάθε πρώτο p, η σειρά*

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

συγκλίνει, και

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

Απόδειξη. Η σύγκλιση της σειράς (;;) είναι άμεση συνέπεια της ανισότητας (3.7.1). Αν $(a,q)=d$ τότε

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

Αφού το άθροισμα

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

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

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

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

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

Συνεπώς,

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

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

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

άρα

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

και η απόδειξη είναι πλήρης. □

Λήμμα 3.7.4. *Αν $s \geqslant 2^k + 1$, τότε*

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

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

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

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

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

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, γνωρίζουμε ότι το γινόμενο Euler (**;;**) συγκλίνει. Ειδικότερα, $\chi_N(p) \neq 0$ για κάθε N και p. Αφού ο $\chi_N(p)$ είναι μη αρνητικός από την (**;;**), συμπεραίνουμε ότι ο $\chi_N(p)$ είναι θετικός πραγματικός αριθμός για κάθε N και p, συνεπώς η ιδιάζουσα σειρά $\mathcal{G}(N)$ είναι θετική. Πάλι, από την (3.7.1),

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

και

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

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

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

για κάθε N και p. Τώρα, η ανισότητα (**;;**) προκύπτει από την σύγκλιση των απειρογινομένων $\prod_p (1 \pm cp^{-1-\delta_4})$. □

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

Έστω p πρώτος, και έστω

$$k = p^r k_0,$$

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

Λήμμα 3.7.5. *Έστω m φυσικός που δεν διαιρείται από τον p. Αν η ισοτιμία $x^k \equiv m \pmod{p^\gamma}$ έχει λύση, τότε η ισοτιμία $y^k \equiv m \pmod{p^h}$ έχει λύση για κάθε $h \geqslant \gamma$.*

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

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

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

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

και

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

Τότε

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

άρα

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

και

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

Συνεπώς, υπάρχει ακέραιος v τέτοιος ώστε

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

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

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

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

και

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

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

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

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

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

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

Λήμμα 3.7.6. *Έστω p πρώτος. Αν υπάρχουν ακέραιοι $a_1, \ldots, a_s$, που δεν διαιρούνται όλοι από τον p, τέτοιοι ώστε*

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

τότε

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

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

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

Αφού η ισοτιμία

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

έχει λύση $x_1 = a_1 \not\equiv 0 \pmod{p}$, από το Λήμμα 3.7.5 βλέπουμε ότι η

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

έχει λύση. Έπεται ότι

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

άρα

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

□

Λήμμα 3.7.7. *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 3.7.6 αρκεί να αποδείξουμε ότι η ισοτιμία

$$a_1^k + \cdots + a_{s-1}^k + 1^k \equiv N \pmod{p^\gamma} \tag{3.7.3}$$

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

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

Σε αυτήν την περίπτωση έχουμε $(N-1, p) = 1$. Αρκεί λοιπόν να δείξουμε ότι αν $(N, p) = 1$ τότε η ισοτιμία (3.7.3) 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 mod p^γ. 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 mod p^γ αν και μόνο αν υπάρχει ακέραιος x τέτοιος ώστε

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

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

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

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

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

υνεπώς υπάρχουν

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

διακεκριμένα υπόλοιπα k-οστών δυνάμεων $\bmod\ p^\gamma$. Έστω $s(N)$ ο μικρότερος φυσικός s για τον οποίο η (3.7.3) έχει λύση, και $C(j)$ το σύνολο όλων των κλάσεων ισοτιμίας $N \bmod p^\gamma$ για τις οποίες $(N,p)=1$ και $s(N)=j$. Ειδικότερα, το $C(1)$ αποτελείται ακριβώς από τα υπόλοιπα k-οστώ δυνάμεων $\bmod\ p^\gamma$. Αν $(m,p)=1$ και $N'=m^kN$, τότε $s(N')=s(N)$. Έπεται ότι τα σύνολα $C(j)$ είναι κλειστά ως προς πολλαπλασιασμό με υπόλοιπα k-οστών δυνάμεων, άρα, αν το $C(j)$ είναι μη κενό τότε $|C(j)| \geqslant (p-1)/(k_0,p-1)$. Έστω n ο μεγαλύτερος φυσικός για τον οποίο το σύνολο $C(n)$ είναι μη κενό. Έστω $j<n$ και έστω N ο μικρότερος φυσικός για τον οποίο $(N,p)=1$ και $s(N)>j$. Αφού ο p είναι περιττός πρώτος, έπεται ότι ο $N-i$ είναι πρώτος προς τον p για $i=1$ ή 2, και $s(N-i)\leqslant j$. Αφού $N=(N-1)+1^k$ και $N=(N-2)+1^k+1^k$, έπεται ότι

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

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

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

άρα

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

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

Έστω $p=2$. Αν ο k είναι περιττός, τότε κάθε περιττός ακέραιος είναι υπόλοιπο k-οστής δύναμης $\bmod\ 2^\gamma$, άρα $s(N)=1$ για όλους τους περιττούς ακεραίους N. Αν ο k είναι άρτιος, τότε $k=2^rk_0$ 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 (3.7.3) λύνεται πάντα αν επιλέξουμε $a_i=1$ για $i=1,\dots,N$ και $a_i=0$ για $i=N+1,\dots,s$. Συνεπώς, $s(N)\leqslant 4k-1$ για όλους τους περιττούς N. Έτσι, ολοκληρώνεται η απόδειξη. □

Θεώρημα 3.7.8. *Υπάρχουν θετικές σταθερές $c_1=c_1(k,s)$ και $c_2=c_2(k,s)$ τέτοιες ώστε*

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

Επιπλέον, για αρκετά μεγάλους φυσικούς N,

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

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

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

για κάθε $N \geqslant 1$. Αφού

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

για κάθε πρώτο p και κάθε N, έπεται ότι

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

και έχουμε ολοκληρώσει την απόδειξη του θεωρήματος. □

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

Θεώρημα 3.7.9 (Hardy-Littlewood)**.** *Έστω $k \geqslant 2$ και $s \geqslant 2^k + 1$. Συμβολίζουμε με $r_{k,s}(N)$ το πλήθος των αναπαραστάσεων του N ως αθροίσματος s το πλήθος k-δυνάμεων φυσικών αριθμών. Υπάρχει σταθερά $\delta = \delta(k,s) > 0$ τέτοια ώστε*

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

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

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

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

Απόδειξη. Θέτουμε $\delta_0 = \min\{1, \delta_1, \delta_2, \delta_3, \nu\delta_4\}$. Από τα Θεωρήματα 3.4.1 έως 3.7.8 έχουμε

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

που $\delta = \delta_0/k$. □

Μέρος II

Το θεώρημα του Freiman

ΚΕΦΑΛΑΙΟ 4

Αθροίσματα συνόλων

4.1 Βασικές εκτιμήσεις

Ορισμός 4.1.1 (αθροίσματα και διαφορές συνόλων)**.** Έστω A και B υποσύνολα μιας αβελιανής ομάδας G. Ορίζουμε

$$A+B=\{a+b \mid a\in A, b\in B\} \text{ και } A-B=\{a-b \mid a\in A, b\in B\}.$$

Εντελώς ανάλογα, αν C είναι ένα τρίτο υποσύνολο της G, θέτουμε

$$A+B+C=\{a+b+c \mid a\in A, b\in B, c\in C\}$$

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 4.1.2 (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 4.1.3 (πρώτη ανισότητα του Ruzsa)**.** *Έστω A,B και C πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Τότε,*

$$|A|\,|B-C|\leqslant|A-B|\,|A-C|. \tag{4.1.1}$$

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 (4.1.1) με $|A|^2\sqrt{|B|\,|C|}$ και παίρνοντας λογαρίθμους έχουμε την *τριγωνική ανισότητα του Ruzsa*:

Πόρισμα 4.1.4 (τριγωνική ανισότητα)**.** *Έστω A, B και C πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Τότε,*

$$\log \frac{|B-C|}{\sqrt{|B|\,|C|}} \leqslant \log \frac{|A-B|}{\sqrt{|A|\,|B|}} + \log \frac{|A-C|}{\sqrt{|A|\,|C|}}. \tag{4.1.2}$$

Ορισμός 4.1.5 (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 4.1.6. 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,

$$d(A,A) \leqslant 2d(A,-A).$$

4.2 Προσθετική ενέργεια

Ορισμός 4.2.1 (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

$$|A|\,|B| \leqslant E(A,B) \leqslant \min\{|A|^2|B|, |B|^2|A|\}. \tag{4.2.1}$$

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 4.2.2. 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 4.2.3 (βασικές ταυτότητες)**.** *Ισχύουν οι ισότητες*

$$E(A,B) = \sum_{x\in G} s(x)^2 = \sum_{x\in G} r(y)^2 = \sum_{z\in G} |A\cap (z+A)|\,|B\cap (z+B)| \tag{4.2.2}$$

και

$$|A|\,|B| = \sum_{y\in A-B} r(y) = \sum_{x\in A+B} s(x). \tag{4.2.3}$$

Απόδειξη. Για την πρώτη ισότητα στην (4.2.2) 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 (4.2.3) 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 4.2.4 (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 4.2.5 (δεύτερη ανισότητα του Ruzsa)**.** *Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Τότε,*

$$d(A,-B) \leqslant 3d(A,B). \tag{4.2.4}$$

Θα χρησιμοποιήσουμε το ακόλουθο λήμμα:

Λήμμα 4.2.6. *Για κάθε $x \in A+B$ ισχύει*

$$s(x) \leqslant \frac{|A-B|^2}{|A+B|}.$$

Απόδειξη του Λήμματος 4.2.6. 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 4.2.5. Από την Πρόταση 4.2.4 και το Λήμμα 4.2.6 έχουμε

$$E(A,B) \leqslant |A|\,|B|\,\max(s) \leqslant |A|\,|B|\,\frac{|A-B|^2}{|A+B|}.$$

Πάλι από την Πρόταση 4.2.4,

$$|A|^2|B|^2 \leqslant |A-B|\,E(A,B).$$

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 4.2.7. Θέτοντας B όπου $-B$ βλέπουμε ότι ισχύει και η $d(A,B) \leqslant 3d(A,-B)$.

4.3 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 4.3.1 (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

$$\max\{|A|, |B|\} \leqslant |A-B| \lessapprox \sqrt{|A|\,|B|}, \tag{4.3.1}$$

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

$$\frac{|A-C|}{\sqrt{|A|\,|C|}} \leqslant \frac{|A-B|}{\sqrt{|A|\,|B|}}\,\frac{|B-C|}{\sqrt{|B|\,|C|}} \lessapprox 1. \tag{4.3.2}$$

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

$$|A \cap C|\,|A-C| \leqslant |(A \cap C) - A|\,|(A \cap C) - C| \leqslant |A-A|\,|C-C|. \tag{4.3.3}$$

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 (4.3.3) παίρνει τη μορφή

$$|A \cap C|\,|A-C| \lessapprox |A|\,|C|. \tag{4.3.4}$$

Από την υπόθεση έχουμε $|A \cap C| \approx |A| \approx |C|$, οπότε η (4.3.4) μας δίνει

$$|A-C| \approx |A| \approx |C|. \tag{4.3.5}$$

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 4.3.2 (ανισότητα τριπλού αθροίσματος)**.** *Έστω A, B και C πεπερασμένα υποσύνολα της αβελιανής ομάδας G. Αν*

$$\max\{d(A,B), d(B,C), d(A,C)\} \leqslant \log K, \tag{4.3.6}$$

τότε

$$|A+B+C| \leqslant K^c \sqrt[3]{|A|}\,\sqrt[3]{|B|}\,\sqrt[3]{|C|}. \tag{4.3.7}$$

Η απόδειξη βασίζεται στην ειδική περίπτωση $n=1$ του ακόλουθου Λήμματος:

Λήμμα 4.3.3. *Υπάρχει σύνολο $S \subseteq A+B$ ώστε*

$$|S| \geqslant \frac{\max\{|A|,|B|\}}{2} \tag{4.3.8}$$

και

$$|A+B+nS| \leqslant \frac{2^n |A+B|^{2n+1}}{|A|^n |B|^n} \tag{4.3.9}$$

για κάθε $n \in \mathbb{N}$.

Απόδειξη του Λήμματος. Ορίζουμε

$$S = \left\{ x \in A+B : s(x) \geqslant \frac{|A|\,|B|}{2|A+B|} \right\}. \tag{4.3.10}$$

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

$$|S| \geqslant \frac{\max\{|A|,|B|\}}{2}. \tag{4.3.11}$$

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 (4.3.9). □

Απόδειξη του Θεωρήματος 4.3.2. 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 4.3.3 (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 4.3.1 έπεται ότι $\sigma(C) \approx 1$. Τότε, από τον ισχυρισμό (v) του θεωρήματος 4.3.1 βλέπουμε ότι $C \sim A+B$. Τότε, $A+B \sim -C$, άρα

$$|A+B+C| \lessapprox \sqrt{|A+B|\,|C|} \approx |A|.$$

□

Πόρισμα 4.3.4 (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. Στην επόμενη παράγραφο θα δούμε την απόδειξη μιας πολύ ισχυρότερης εκδοχής του.

4.4 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 4.4.1 (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 4.4.2. *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 4.4.3 (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 4.4.4. 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 5

Γεωμετρία των αριθμών

5.1 Πλέγματα

Ένα υποσύνολο Λ του $\mathbb{R}^d$, $d \geqslant 2$, λέγεται *πλέγμα* αν υπάρχουν γραμμικά ανεξάρτητα διανύσματα $u_1, \ldots, u_d \in \mathbb{R}^d$ ώστε

$$\Lambda = \{x \in \mathbb{R}^d : x = m_1 u_1 + \ldots + m_d u_d, m_i \in \mathbb{Z}\}.$$

Τότε λέμε ότι το $\{u_1, \ldots, u_d\}$ είναι μια *βάση* του πλέγματος Λ. Ένα πλέγμα μπορεί να έχει περισότερες από μία βάσεις (για την ακρίβεια, θα δούμε ότι κάθε πλέγμα έχει άπειρες το πλήθος). Παρατηρήστε ότι ένα υποσύνολο Λ του $\mathbb{R}^d$ είναι πλέγμα αν και μόνο αν υπάρχει $T \in GL(d)$ ώστε $\Lambda = T(\mathbb{Z}^d)$.

Πρόταση 5.1.1. *Κάθε πλέγμα Λ στον $\mathbb{R}^d$ είναι διακριτή προσθετική υποομάδα του $\mathbb{R}^d$. Δηλαδή, υπάρχει $r > 0$ ώστε $rB_2^d \cap \Lambda = \{0\}$.*

Απόδειξη. Έστω $\Lambda = T(\mathbb{Z}^d)$, $T \in GL(d)$. Αν $x, y \in \Lambda$ τότε $x - y \in \Lambda$, άρα το Λ είναι προσθετική υποομάδα του $\mathbb{R}^d$. Επίσης, αν ορίσουμε $Q = \{x \in \mathbb{R}^d : |x_i| < 1\}$, τότε $\mathbb{Z}^d \cap Q = \{0\}$. Αφού ο T είναι ένα προς ένα,

$$\Lambda \cap T(Q) = T(\mathbb{Z}^d \cap Q) = \{0\}.$$

Όμως το $T(Q)$ είναι ανοικτό υποσύνολο του $\mathbb{R}^d$ και $0 \in T(Q)$, άρα υπάρχει $r > 0$ ώστε $rB_2^d \subset T(Q)$. Έπεται ότι $rB_2^d \cap \Lambda = \{0\}$. □

Άμεσες συνέπειες του ορισμού της διακριτής προσθετικής ομάδας είναι οι εξής:

(i) Αν $rB_2^d \cap \Lambda = \{0\}$, τότε για κάθε $u \in \Lambda$ ισχύει $B(u, r) \cap \Lambda = \{u\}$.

(ii) Για κάθε $R > 0$, η RB_2^d 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^d, 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 $0 \neq x_{k_m} - x_{k_n} \in rB_2^d \cap \Lambda$. Δηλαδή, το Λ δεν θα ήταν διακριτή προσθετική υποομάδα του $\mathbb{R}^d$.

Πρόταση 5.1.2. *Ένα υποσύνολο Λ του $\mathbb{R}^d$ είναι πλέγμα αν και μόνο αν περιέχει d γραμμικώς ανεξάρτητα διανύσματα και είναι διακριτή προσθετική υποομάδα του $\mathbb{R}^d$.*

Απόδειξη. Η μία κατεύθυνση δίνεται από την Πρόταση 5.1.1. Για την άλλη κατεύθυνση, υποθέτουμε ότι Λ είναι μια διακριτή προσθετική υποομάδα του $\mathbb{R}^d$, που περιέχει τα γραμμικά ανεξάρτητα διανύσματα $x_1, \ldots, x_d$. Θα κατασκευάσουμε μία βάση του Λ, δηλαδή ένα σύνολο $\{u_1, \ldots, u_d\}$ γραμμικά ανεξάρτητων διανυσμάτων στο Λ με την ιδιότητα: κάθε $v \in \Lambda$ γράφεται μονοσήμαντα στη μορφή $v = m_1u_1 + \ldots + m_du_d$, όπου $m_1, \ldots, m_d \in \mathbb{Z}$.

Τα $u_1, \ldots, u_d$ 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 $k \leqslant d$ 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 $u_1, \ldots, u_k$:

$$\Lambda_k := \Lambda \cap \langle x_1, \ldots, x_k \rangle = \{m_1u_1 + \ldots + m_ku_k : m_i \in \mathbb{Z}\}.$$

Με μια τέτοια κατασκευή, τα u_i είναι γραμμικά ανεξάρτητα και, για $k = d$, έχουμε

$$\Lambda = \{x \in \mathbb{R}^d : x = m_1u_1 + \ldots + m_du_d, m_i \in \mathbb{Z}\},$$

δηλαδή το Λ είναι πλέγμα.

Για την επιλογή του u_{k+1} θεωρούμε το παραλληλεπίπεδο

$$P = \{x = a_1u_1 + \ldots + a_ku_k + bx_{k+1}, 0 \leqslant a_i < 1, 0 < b \leqslant 1\},$$

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

$$\Lambda_{k+1} := \Lambda \cap \langle x_1, \ldots, x_{k+1} \rangle = \{m_1u_1 + \ldots + m_{k+1}u_{k+1} : m_i \in \mathbb{Z}\}.$$

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 $x = t_1u_1 + \ldots + t_ku_k + t_{k+1}u_{k+1}$ για κάποιους $t_1, \ldots, t_{k+1} \in \mathbb{R}$. Θέτουμε $\{z\} = z - [z]$ το κλασματικό μέρος του z, και θεωρούμε το

$$x' = \{t_1\}u_1 + \ldots + \{t_k\}u_k + \{t_{k+1}\}u_{k+1} \in \Lambda.$$

Τότε,

$$\begin{aligned} x' &= \{t_1\}u_1 + \ldots + \{t_k\}u_k + \{t_{k+1}\}\left(\sum_{i=1}^{k} a_i u_i + b x_{k+1}\right) \\ &= t_1' u_1 + \ldots + t_k' u_k + \{t_{k+1}\} b x_{k+1} \in \Lambda, \end{aligned}$$

άρα, αν $0 < \{t_{k+1}\}$ τότε

$$x'' = \{t_1'\}u_1 + \ldots + \{t_k'\}u_k + \{t_{k+1}\}bx_{k+1} \in \Lambda \cap P,$$

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,

$$x' = \{t_1\}u_1 + \ldots \{t_k\}u_k \in \Lambda \cap \langle x_1, \ldots, x_k\rangle,$$

και, από την επαγωγική μας υπόθεση, πρέπει να έχουμε $t_1, \ldots, t_k \in \mathbb{Z}$. Αυτό αποδεικνύει την $(*)$ και, επαγωγικά, το θεώρημα. □

Παρατήρηση 5.1.3. Η απόδειξη της Πρότασης δίνει ταυτόχρονα έναν τρόπο να περνάμε από ένα γραμμικά ανεξάρτητο υποσύνολο $\{x_1, \ldots, x_d\}$ ενός πλέγματος Λ σε βάση $\{u_1, \ldots, u_d\}$ του Λ, με την ιδιότητα

$$\langle u_1, \ldots, u_k\rangle = \langle x_1, \ldots, x_k\rangle, \qquad 1 \leqslant k \leqslant d.$$

Ορίζουσα πλέγματος

Έστω Λ ένα πλέγμα στον $\mathbb{R}^d$ και έστω $u_1, \ldots, u_d$ μια βάση του. Το παραλληλεπίπεδο

$$Q = \{\sum_{i=1}^{d} a_i u_i : 0 \leqslant a_i < 1\}$$

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 5.1.4. *Έστω Λ ένα πλέγμα στον $\mathbb{R}^d$, και έστω P, Q δύο θεμελιώδη παραλληλεπίπεδα του Λ. Τότε, $|P| = |Q|$.*

Απόδειξη. Έστω $\{u_1, \ldots, u_d\}$ και $\{v_1, \ldots, v_d\}$ 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

$$u_i = \sum_{j=1}^{d} m_{ij} v_j, \quad v_i = \sum_{j=1}^{d} l_{ij} u_j,$$

όπου $M = (m_{ij})$ και $L = (l_{ij})$ πίνακες με ακέραιες συντεταγμένες. Τότε $U = VM^*$ και $V = UL^*$, 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

$$|P| = |\det U| = |\det M| \cdot |\det V| = |\det V| = |Q|.$$

□

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 $\mathbb{R}^d$, και $u_1, \ldots, u_d \in \Lambda$, τότε τα $u_1, \ldots, u_d$ είναι βάση του Λ αν και μόνο αν

$$|\det(u_1, \ldots, u_d)| = \det \Lambda.$$

Η μία κατεύθυνση είναι προφανής από τον ορισμό της $\det \Lambda$. Για την αντίστροφη κατεύθυνση, έστω $u_1, \ldots, u_d \in \Lambda$ με $|\det(u_1, \ldots, u_d)| = \det \Lambda$. Αφού $\det \Lambda > 0$, τα u_i είναι γραμμικά ανεξάρτητα. Θεωρούμε μία βάση V του Λ, και γράφουμε $U = VM^*$ και $V = UL^*$. 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 $V = UL^*$ 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 $\mathbb{R}^d$, $d \geqslant 2$:

Πρόταση 5.1.5. *Αν $x = (x_1, \ldots, x_d) \in \mathbb{Z}^d$ και ο μέγιστος κοινός διαιρέτης των $x_1, \ldots, x_d$ είναι 1, τότε το x επεκτείνεται σε βάση του $\mathbb{Z}^d$.*

Απόδειξη. Μπορούμε να βρούμε $y_2, \ldots, y_d \in \mathbb{Z}^d$ ώστε τα $x, y_2, \ldots, y_d$ να είναι γραμμικά ανεξάρτητα: αφού $x \neq 0$, υπάρχει $i_0 \leqslant d$ ώστε $x_{i_0} \neq 0$, οπότε μπορούμε να πάρουμε σαν y_j τα διανύσματα e_i, $i \neq i_0$.

Κατόπιν κατασκευάζουμε βάση $\{u_1, \ldots, u_d\}$ όπως στην Πρόταση 5.1.2, ξεκινώντας από τα $x, y_2, \ldots, y_d$. 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 $x_1, \ldots, x_d$ έχουν μέγιστο κοινό διαιρέτη τη μονάδα. □

Πόρισμα 5.1.6. *Κάθε πλέγμα Λ στον $\mathbb{R}^d$, $d \geqslant 2$, έχει άπειρες το πλήθος διαφορετικές βάσεις.*

Απόδειξη. Αρκεί να εξετάσουμε την περίπτωση $\Lambda = \mathbb{Z}^d$. Υπάρχουν άπειρες το πλήθος d-άδες μη μηδενικών ακεραίων $x_1, \ldots, x_d$ που έχουν μέγιστο κοινό διαιρέτη τη μονάδα. Κάθε μία από αυτές ανήκει σε μια βάση του $\mathbb{Z}^d$, από την Πρόταση 5.1.5. Άρα, το $\mathbb{Z}^d$ έχει άπειρες διαφορετικές βάσεις. □

Το τελευταίο αποτέλεσμα αυτής της παραγράφου δίνει μία σημαντική ιδιότητα του θεμελιώδους παραλληλεπιπέδου (την οποία θα χρησιμοποιήσουμε αρκετές φορές στη συνέχεια):

Πρόταση 5.1.7. *Έστω Λ ένα πλέγμα στον $\mathbb{R}^d$, $\{u_1, \ldots, u_d\}$ μια βάση του Λ, και $Q = \{a_1u_1 + \ldots + a_du_d : 0 \leqslant a_i < 1\}$ το αντίστοιχο θεμελιώδες παραλληλεπίπεδο. Τότε,*

$$\mathbb{R}^d = Q \oplus \Lambda.$$

Δηλαδή, οι μεταφορές του Q κατά τα σημεία του Λ, καλύπτουν τον $\mathbb{R}^d$ χωρίς να επικαλύπτονται.

Απόδειξη. Έστω $x \in \mathbb{R}^d$. Τα u_i είναι βάση του $\mathbb{R}^d$, άρα μπορούμε να γράψουμε $x = \sum_{i=1}^d t_iu_i$ για κάποιους $t_i \in \mathbb{R}$. Θεωρούμε τα διανύσματα

$$y = \sum_{i=1}^d \{t_i\}u_i, \quad z = \sum_{i=1}^d [t_i]u_i.$$

Τότε, $z \in \Lambda$, $y \in Q$, και

$$x = y + z \in Q + \Lambda.$$

Κάθε $x \in \mathbb{R}^d$ γράφεται με μοναδικό τρόπο σε αυτή τη μορφή: Αν για κάποιο $x \in \mathbb{R}^d$ είχαμε $x = y + z = y_1 + z_1$ με $y, y_1 \in Q$, και $z, z_1 \in \Lambda$, τότε θα είχαμε $y - y_1 \in \Lambda$, δηλαδή

$$y - y_1 = \sum_{i=1}^d b_iu_i, \qquad b_i \in \mathbb{Z}.$$

Όμως, $|b_i| = |a_i(y) - a_i(y_1)| < 1$. Έπεται ότι $b_i = 0$ για κάθε $i \leqslant d$. Οπότε $y = y_1$ και $z = z_1$, που αποδεικνύει το ζητούμενο. □

Υποπλέγματα

Έστω Λ ένα πλέγμα στον $\mathbb{R}^d$ 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 μιάς αβελιανής ομάδας, 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 5.1.8. *Έστω $V = \{v_1, \ldots, v_d\}$ μία βάση του Λ_0. Αν $Q = \{\sum_{i=1}^d a_iv_i : 0 \leqslant a_i < 1\}$ 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, $y_1 - y_2 \in \{\sum_{i=1}^{d} a_i v_i : \ |a_i| < 1\}$, 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 5.1.7, 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 5.1.9. *Έστω Λ_0 ένα υποπλέγμα του πλέγματος Λ στον $\mathbb{R}^d$. Υπάρχουν βάσεις $U = \{u_1, \ldots, u_d\}$ του Λ και $V = \{v_1, \ldots, v_d\}$ του Λ_0, ώστε*

$$v_i = m_i u_i, \quad 1 = i, \ldots, d$$

και

$$m_i \mid m_{i+1}, \quad i = 1, \ldots, d-1.$$

Απόδειξη. Έστω $U = \{u_i\}$ και $V = \{v_i\}$ δύο βάσεις των Λ και Λ_0 αντίστοιχα. Κάθε $v_i \in V$ γράφεται μονοσήμαντα στη μορφή

$$v_i = m_{i1} u_1 + \cdots + m_{id} u_d, \quad m_{ij} \in \mathbb{Z}.$$

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

$$V = UM^*.$$

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 $V_1 = \{v_1, \ldots, -v_i, \ldots, v_d\}$.

(δ) Αν πολλαπλασιάσουμε την i στήλη με -1, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις $U_1 = \{u_1, \ldots, -u_i, \ldots, u_d\}$ 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 $V_1 = \{v_1, \ldots, v_i + sv_j, \ldots, v_d\}$.

(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 $U_1 = \{u_1, \ldots, u_i - su_j, \ldots, u_d\}$ 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 $i, j = 1, \dots d$. 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 $i, j = 1, \dots, d$, 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 $m_{1j} = m_{i1} = 0$, $i, j = 2, \dots, d$. 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 d βήματα, θα φτάσουμε στη ζητούμενη μορφή. □

Η χρησιμότητα της κανονικής μορφής του Smith φαίνεται από το επόμενο θεώρημα.

Θεώρημα 5.1.10. *Έστω Λ_0 ένα υποπλέγμα του πλέγματος Λ στον $\mathbb{R}^d$. 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 5.1.8, 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 5.1.9, μπορούμε να επιλέξουμε βάσεις U, V ώστε

$$v_i = m_i u_i, \quad m_i \in \mathbb{Z}, \ \ i = 1, \dots, d.$$

Τότε, είναι φανερό ότι

$$\det M(U,V) = m_1 m_2 \dots m_d.$$

Απομένει να μετρήσουμε το πλήθος των σημείων του Λ που ανήκουν στο Q. Όμως, λόγω της σχέσεως $v_i = m_i u_i$ έχουμε ότι, για κάθε $i = 1, \dots, d$, στο ευθύγραμμο τμήμα $[0, v_i)$ υπάρχουν m_i

το πλήθος σημεία του Λ. Άρα στο Q θα έχουμε $m_1 m_2 \dots m_d$ σημεία του Λ, τα $t_1 v_1 + \dots + t_d v_d$, $t_i \in \{0, 1, \dots, m_i - 1\}$. Αυτό αποδεικνύει το ζητούμενο. □

Παρατήρηση. Το Θεώρημα 5.1.10 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 $\mathbb{Z}^d$. Αν $v_1, \dots, v_d$ είναι γραμμικώς ανεξάρτητα διανύσματα του $\mathbb{R}^d$ 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 $\mathbb{Z}^d$ που παράγουν τα v_i, από το Θεώρημα 2.3.2 έχουμε

$$|Q| = |\det \Lambda_0| = |\mathbb{Z}^d : \Lambda_0| = |\mathbb{Z}^d \cap Q|.$$

Δυϊκό πλέγμα

Έστω Λ ένα πλέγμα στον $\mathbb{R}^d$. Το σύνολο

$$\Lambda^* := \{y \in \mathbb{R}^d : \forall x \in \Lambda, \ \langle x, y\rangle \in \mathbb{Z}\}$$

ονομάζεται **δυϊκό πλέγμα** του Λ.

Στην επόμενη πρόταση αποδεικνύουμε ότι το Λ^* είναι όντως πλέγμα, και περιγράφουμε το Λ^* συναρτήσει του Λ:

Πρόταση 5.1.11. *Το Λ^* είναι πλέγμα στον $\mathbb{R}^d$. Αν $u_1, \dots, u_d$ είναι μία βάση του Λ, τότε τα διανύσματα $u_1^*, \dots, u_d^*$ που ορίζονται από τις*

$$\langle u_i, u_j^*\rangle = \delta_{ij}, \quad i, j = 1, \dots, d$$

αποτελούν βάση του Λ^*.

Απόδειξη. Παρατηρούμε ότι

$$(\mathbb{Z}^d)^* = \mathbb{Z}^d.$$

Πράγματι, αν $x = (x_1, \dots, x_d) \in (\mathbb{Z}^d)^*$, τότε $x_i = \langle x, e_i\rangle \in \mathbb{Z}$ για κάθε $i = 1, \dots, d$, άρα $x \in \mathbb{Z}^d$. Αντιστρόφως, αν $x \in \mathbb{Z}^d$ τότε, προφανώς $\langle x, y\rangle \in \mathbb{Z}$ για κάθε $y \in \mathbb{Z}^d$, δηλαδή $x \in (\mathbb{Z}^d)^*$.

(α) Δείχνουμε πρώτα ότι το Λ^* είναι πλέγμα. Υπάρχει $T \in GL(d)$ ώστε $\Lambda = T(\mathbb{Z}^d)$. Τότε,

$$\begin{aligned} x \in \Lambda^* &\iff \forall y \in \Lambda \ \ \langle x, y\rangle \in \mathbb{Z} \\ &\iff \forall z \in \mathbb{Z}^d \ \ \langle x, Tz\rangle \in \mathbb{Z} \\ &\iff \forall z \in \mathbb{Z}^d \ \ \langle T^* x, z\rangle \in \mathbb{Z} \\ &\iff T^* x \in (\mathbb{Z}^d)^* = \mathbb{Z}^d \\ &\iff x \in T^{-*}(\mathbb{Z}^d). \end{aligned}$$

Όμως, $T^{-*} \in GL(d)$. Άρα, το $\Lambda^* = T^{-*}(\mathbb{Z}^d)$ είναι πλέγμα.

(β) Για τον δεύτερο ισχυρισμό, ας υποθέσουμε ότι $\{u_1, \dots, u_d\}$ είναι μια βάση του Λ. Θεωρούμε τον $T \in GL(d)$ που ορίζεται από τις $T(e_i) = u_i$, $i = 1, \dots, d$. Τότε, $\Lambda = T(\mathbb{Z}^d)$. Αν θέσουμε $u_j^* = T^{-*}(e_j)$, τότε το $\{u_1^*, \dots, u_d^*\}$ είναι βάση του $T^{-*}(\mathbb{Z}^d) = \Lambda^*$, και

$$\langle u_i, u_j^* \rangle = \langle Te_i, T^{-*}e_j \rangle = \langle T^{-1}Te_i, e_j \rangle = \langle e_i, e_j \rangle = \delta_{ij}.$$

□

Η βάση $\{u_1^*, \dots, u_d^*\}$ του Λ^* που ορίσαμε στην Πρόταση 2.5.1 ονομάζεται **δυϊκή βάση** της $\{u_1, \dots, u_d\}$.

Λ-υπόχωροι

Ορισμός 5.1.12. (α) Έστω Λ ένα πλέγμα στον $\mathbb{R}^d$. Ένας k-διάστατος γραμμικός υπόχωρος F του $\mathbb{R}^d$ ονομάζεται **Λ-υπόχωρος** αν το $F \cap \Lambda$ είναι πλέγμα στον F. Δηλαδή, αν υπάρχουν $v_1, \dots, v_k \in F$ ώστε

$$F \cap \Lambda = \{m_1 v_1 + \dots + m_k v_k : m_i \in \mathbb{Z}\}.$$

(β) Έστω F ένας k-διάστατος Λ-υπόχωρος του $\mathbb{R}^d$. 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 5.1.13. *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 d γραμμικά ανεξάρτητα διανύσματα, επομένως μπορούμε να βρούμε $u_{k+1}, \dots, u_d \in \Lambda$ ώστε τα $v_1, \dots, v_k, u_{k+1}, \dots, u_d$ να είναι γραμμικά ανεξάρτητα. Ξεκινώντας από αυτά τα διανύσματα, κατασκευάζουμε βάση του Λ όπως στο Θεώρημα ;;. 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 5.1.14. Έστω F ένας Λ-υπόχωρος. Ορίζουμε

$$F^\perp = \{y \in \mathbb{R}^d : \langle x, y \rangle = 0, \ \ \forall x \in F\}.$$

Θεώρημα 5.1.15. *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 2.5.1, την επεκτείνουμε σε βάση $\{v_1, \dots, v_k, v_{k+1}, \dots, v_d\}$ του Λ. Θεωρούμε τη δυϊκή βάση $\{u_1, \dots, u_d\}$ του Λ^*. Τότε, για κάθε $k+1 \leqslant j \leqslant d$ έχουμε

$$\langle v_i, u_j \rangle = 0, \quad i = 1, \dots, k,$$

άρα $u_j \in F^\perp$, $j = k+1, \dots, d$. Τα $u_{k+1}, \dots, u_n$ είναι γραμμικά ανεξάρτητα και ανήκουν στον $F^\perp \cap \Lambda^*$, επομένως ο $F^\perp$ είναι Λ^*-υπόχωρος. □

5.2 Κυρτά σώματα

Κυρτό σώμα στον $\mathbb{R}^d$ είναι ένα μη κενό, κυρτό και συμπαγές υποσύνολο K του $\mathbb{R}^d$, 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 κατά Minkowski** δύο μη κενών υποσυνόλων A και B του $\mathbb{R}^d$ 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.

Για κάθε νόρμα $\|\cdot\|$ στον $\mathbb{R}^d$, η μοναδιαία μπάλα $B_X = \{x \in \mathbb{R}^d : \|x\| \leqslant 1\}$ του χώρου με νόρμα $X = (\mathbb{R}^d, \|\cdot\|)$ είναι ένα συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$. Αντίστροφα, αν K είναι ένα συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$ τότε η συνάρτηση

$$\|x\|_K = \min\{\lambda \geqslant 0 : x \in \lambda K\}$$

είναι νόρμα, για την οποία ισχύει $\|x\|_K \leqslant 1$ αν και μόνο αν $x \in K$. Η ύπαρξη του λεγόμενου *συναρτησοειδούς του Minkowski* δείχνει ότι, με μια έννοια, η μελέτη των συμμετρικών κυρτών σωμάτων στον $\mathbb{R}^d$ είναι ισοδύναμη με τη μελέτη των νορμών πάνω στον $\mathbb{R}^d$.

Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$. Το **πολικό σώμα** του K είναι το

$$K^\circ = \{y \in \mathbb{R}^d : \forall x \in K,\ |\langle x, y\rangle| \leqslant 1\}.$$

Θεωρούμε το χώρο $X = (\mathbb{R}^d, \|\cdot\|_K)$, και το δυϊκό του χώρο X^*. Τα γραμμικά συναρτησοειδή $f : X \to \mathbb{R}$ αναπαρίστανται από $y_f \in \mathbb{R}^d$: για κάθε $f \in X^*$ υπάρχει μοναδικό $y_f \in \mathbb{R}^d$ ώστε

$$f(x) = \langle y, x\rangle, \quad x \in \mathbb{R}^d,$$

και αντίστροφα κάθε $y \in \mathbb{R}^d$ ορίζει $f_y \in X^*$ με τον ίδιο τρόπο. Μπορούμε λοιπόν να ταυτίσουμε (ως γραμμικό χώρο) τον X^* με τον $\mathbb{R}^d$. Μεταφέρουμε τη νόρμα του X^* στον $\mathbb{R}^d$, ορίζοντας

$$\|y\|_* = \|f_y\|_{X^*} = \max_{x \in B_X} |f_y(x)| = \max\{|\langle y, x\rangle| : x \in K\}.$$

Τότε, η μοναδιαία μπάλα του $(\mathbb{R}^d, \|\cdot\|_*)$ είναι ακριβώς το K°. Πράγματι,

$$K^\circ = \{y \in \mathbb{R}^d : \max_{x \in K} |\langle y, x\rangle| \leqslant 1\} = \{y \in \mathbb{R}^d : \|y\|_* \leqslant 1\}.$$

Έχουμε λοιπόν αποδείξει το εξής:

Πρόταση 5.2.1. *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$ και έστω $X = (\mathbb{R}^d, \|\cdot\|_K)$. Τότε, το K° είναι η μοναδιαία μπάλα του δυϊκού χώρου του X.*

Από τον ορισμό του πολικού σώματος, και από τον χαρακτηρισμό του που μάς δίνει η προηγούμενη Πρόταση, μπορούμε εύκολα να αποδείξουμε τις παρακάτω βασικές ιδιότητές του:

Πρόταση 5.2.2. *Έστω K, K_1 συμμετρικά κυρτά σώματα στον $\mathbb{R}^d$. Τότε,*
(α) Αν $K \subseteq K_1$, τότε $K_1^\circ \subseteq K^\circ$.
(β) $(K^\circ)^\circ = K$.
(γ) Αν $T \in GL(d)$, τότε $(TK)^\circ = T^{-*}K^\circ$.
(δ) $|K||K^\circ| = |TK||(TK)^\circ|$.

Η ανισότητα Brunn-Minkowski

Η ανισότητα Brunn-Minkowski συνδέει τον όγκο με την πράξη της πρόσθεσης κατά Minkowski.

Θεώρημα 5.2.3. *(**Ανισότητα Brunn-Minkowski**). Έστω A και B συμπαγή, μη κενά υποσύνολα του $\mathbb{R}^d$. Τότε,*

$$|A+B|^{1/d} \geqslant |A|^{1/d} + |B|^{1/d}.$$

Η ανισότητα Brunn-Minkowski γιά κυρτά σώματα στον $\mathbb{R}^d$ συχνά διατυπώνεται ως εξής:

Πόρισμα 5.2.4. *Έστω K_1, K_2 κυρτά σώματα στον $\mathbb{R}^d$. Γιά κάθε $\lambda \in (0,1)$ ισχύει*

$$|\lambda K_1 + (1-\lambda)K_2|^{1/d} \geqslant \lambda |K_1|^{1/d} + (1-\lambda)|K_2|^{1/d}.$$

Δηλαδή, η συνάρτηση $f : [0,1] \to \mathbb{R}$ με $f(\lambda) = |\lambda K_1 + (1-\lambda)K_2|^{1/d}$ είναι κοίλη.

Μια άλλη συνέπεια της ανισότητας Brunn-Minkowski είναι η ακόλουθη ανισότητα (η οποία είναι *ανεξάρτητη της διάστασης*):

Πόρισμα 5.2.5. *Έστω A, B συμπαγή, μη κενά υποσύνολα του $\mathbb{R}^d$. Γιά κάθε $\lambda \in (0,1)$ έχουμε*

$$|\lambda A + (1-\lambda)B| \geqslant |A|^\lambda |B|^{1-\lambda}.$$

Απόδειξη. Η συνάρτηση log είναι κοίλη, κι αυτό έχει σαν συνέπεια την

$$x^\lambda y^{1-\lambda} \leqslant \lambda x + (1-\lambda)y$$

γιά κάθε $x, y > 0$ και $\lambda \in (0,1)$. Από την ανισότητα Brunn-Minkowski παίρνουμε

$$|\lambda A + (1-\lambda)B| \geqslant [\lambda |A|^{1/d} + (1-\lambda)|B|^{1/d}]^d \geqslant [|A|^{\lambda/d}|B|^{(1-\lambda)/d}]^d = |A|^\lambda |B|^{1-\lambda}.$$

□

Θα αποδείξουμε την ανισότητα Brunn–Minkowski χρησιμοποιώντας τη συναρτησιακή ανισότητα των Prékopa και Leindler.

Θεώρημα 5.2.6. *Έστω $f, g, h : \mathbb{R}^d \to \mathbb{R}^+$ τρείς μετρήσιμες συναρτήσεις και $\lambda \in (0,1)$. Υποθέτουμε ότι οι f και g είναι ολοκληρώσιμες και ότι για κάθε $x, y \in \mathbb{R}^d$*

$$h(\lambda x + (1-\lambda)y) \geqslant f(x)^\lambda g(y)^{1-\lambda}.$$

Τότε,

$$\int_{\mathbb{R}^d} h \geqslant \left(\int_{\mathbb{R}^d} f\right)^\lambda \left(\int_{\mathbb{R}^d} g\right)^{1-\lambda}.$$

Απόδειξη. Θα δείξουμε την ανισότητα με επαγωγή ως προς τη διάσταση d.

(α) $d = 1$: Μπορούμε να υποθέσουμε ότι οι f και g είναι συνεχείς και γνήσια θετικές. Ορίζουμε $x, y : (0,1) \to \mathbb{R}$ μέσω των

$$\int_{-\infty}^{x(t)} f = t \int f \quad , \quad \int_{-\infty}^{y(t)} g = t \int g.$$

Σύμφωνα με τις υποθέσεις μας οι x, y είναι παραγωγίσιμες, και για κάθε $t \in (0,1)$ έχουμε

$$x'(t) f(x(t)) = \int f \quad , \quad y'(t) g(y(t)) = \int g.$$

Ορίζουμε $z : (0,1) \to \mathbb{R}$ με

$$z(t) = \lambda x(t) + (1-\lambda) y(t).$$

Οι x και y είναι γνήσια αύξουσες. Επομένως, η z είναι κι αυτή γνήσια αύξουσα. Από την ανισότητα αριθμητικού-γεωμετρικού μέσου,

$$z'(t) = \lambda x'(t) + (1-\lambda) y'(t) \geqslant (x'(t))^{\lambda} (y'(t))^{1-\lambda}.$$

Μπορούμε λοιπόν να εκτιμήσουμε το ολοκλήρωμα της h κάνοντας την αλλαγή μεταβλητών $s = z(t)$:

$$\begin{aligned} \int h(s)ds &= \int_0^1 h(z(t)) z'(t) dt \\ &\geqslant \int_0^1 h(\lambda x(t) + (1-\lambda) y(t)) (x'(t))^{\lambda} (y'(t))^{1-\lambda} dt \\ &\geqslant \int_0^1 f^{\lambda}(x(t)) g^{1-\lambda}(y(t)) \left(\frac{\int f}{f(x(t))} \right)^{\lambda} \left(\frac{\int g}{g(y(t))} \right)^{1-\lambda} dt \\ &= \left(\int f \right)^{\lambda} \left(\int g \right)^{1-\lambda}. \end{aligned}$$

(β) *Επαγωγικό βήμα:* Υποθέτουμε ότι $d \geqslant 2$ και ότι το Θεώρημα έχει αποδειχθεί για $k \in \{1, \dots, d-1\}$. Έστω f, g, h όπως στο Θεώρημα. Για κάθε $s \in \mathbb{R}$ ορίζουμε $h_s : \mathbb{R}^{d-1} \to \mathbb{R}^+$ με $h_s(w) = h(w,s)$, και με ανάλογο τρόπο ορίζουμε $f_s, g_s : \mathbb{R}^{d-1} \to \mathbb{R}^+$. Από την υπόθεση του θεωρήματος για τις f, g και h έπεται ότι, αν $x, y \in \mathbb{R}^{d-1}$ και $s_0, s_1 \in \mathbb{R}$ τότε

$$h_{\lambda s_1 + (1-\lambda) s_0}(\lambda x + (1-\lambda) y) \geqslant f_{s_1}(x)^{\lambda} g_{s_0}(y)^{1-\lambda},$$

και η επαγωγική υπόθεση μας δίνει

$$\begin{aligned} H(\lambda s_1 + (1-\lambda) s_0) &:= \int_{\mathbb{R}^{d-1}} h_{\lambda s_1 + (1-\lambda) s_0} \\ &\geqslant \left(\int_{\mathbb{R}^{d-1}} f_{s_1} \right)^{\lambda} \left(\int_{\mathbb{R}^{d-1}} g_{s_0} \right)^{1-\lambda} =: F^{\lambda}(s_1) G^{1-\lambda}(s_0). \end{aligned}$$

Εφαρμόζοντας τώρα ξανά την επαγωγική υπόθεση για $d = 1$ στις συναρτήσεις F, G και H, παίρνουμε

$$\int h = \int_{\mathbb{R}} H \geqslant \left(\int_{\mathbb{R}} F \right)^{\lambda} \left(\int_{\mathbb{R}} G \right)^{1-\lambda} = \left(\int f \right)^{\lambda} \left(\int g \right)^{1-\lambda}.$$

□

Χρησιμοποιώντας την ανισότητα Prékopa–Leindler μπορούμε να αποδείξουμε την ανισότητα Brunn–Minkowski:

Απόδειξη του Πορίσματος 2.2.3. Έστω K, T συμπαγή μη κενά υποσύνολα του $\mathbb{R}^d$, και $\lambda \in (0,1)$. Ορίζουμε $f = \chi_K$, $g = \chi_T$, και $h = \chi_{\lambda K+(1-\lambda)T}$. Εύκολα ελέγχουμε ότι ικανοποιούνται οι υποθέσεις του θεωρήματος 2.3.4. Πράγματι, αν $x \notin K$ ή $y \notin T$ τότε

$$h(\lambda x + (1-\lambda)y) \geqslant 0 = [f(x)]^\lambda [g(y)]^{1-\lambda},$$

ενώ αν $x \in K$ και $y \in T$ τότε $\lambda x + (1-\lambda)y \in \lambda K + (1-\lambda)T$, άρα

$$h(\lambda x + (1-\lambda)y) = 1 = [f(x)]^\lambda [g(y)]^{1-\lambda}.$$

Εφαρμόζοντας την ανισότητα Prékopa-Leindler παίρνουμε

$$(*) \qquad |\lambda K + (1-\lambda)T| = \int h \geqslant \left(\int f\right)^\lambda \left(\int g\right)^{1-\lambda} = |K|^\lambda |T|^{1-\lambda}.$$

Θεωρούμε τώρα K και T όπως στο Θεώρημα 2.2.1 (με $|K| > 0$ και $|T| > 0$, αλλιώς δεν έχουμε τίποτα να δείξουμε), και ορίζουμε

$$K_1 = |K|^{-1/d} K \quad , \quad T_1 = |T|^{-1/d} T \quad , \quad \lambda = \frac{|K|^{1/d}}{|K|^{1/d} + |T|^{1/d}}.$$

Τα K_1 και T_1 έχουν όγκο 1, οπότε από την $(*)$ παίρνουμε

$$(**) \qquad |\lambda K_1 + (1-\lambda)T_1| \geqslant 1.$$

Ομως,

$$\lambda K_1 + (1-\lambda)T_1 = \frac{K+T}{|K|^{1/d} + |T|^{1/d}},$$

επομένως η $(**)$ παίρνει την μορφή

$$|K+T| \geqslant \left(|K|^{1/n} + |T|^{1/n}\right)^n$$

και έπεται το ζητούμενο. □

Το θεώρημα του John

Ελλειψοειδές στον $\mathbb{R}^d$ είναι ένα κυρτό σώμα της μορφής

$$(*) \qquad E = \left\{ x \in \mathbb{R}^d : \sum_{i=1}^d \frac{\langle x, v_i\rangle^2}{\alpha_i^2} \leqslant 1 \right\},$$

όπου $\{v_i\}_{i \leqslant d}$ είναι ορθοκανονική βάση του $\mathbb{R}^d$, και $\alpha_1, \ldots, \alpha_d$ είναι θετικοί πραγματικοί αριθμοί (οι διευθύνσεις και τα μήκη των ημιαξόνων του E αντίστοιχα). Το $E \subseteq \mathbb{R}^d$ είναι ελλειψοειδές αν και μόνο αν υπάρχει $T \in GL(d)$ τέτοιος ώστε $E = T(B_2^d)$.

Θεωρούμε τώρα ένα συμμετρικό κυρτό σώμα K στον $\mathbb{R}^d$ και την οικογένεια $\mathcal{E}(K)$ όλων των ελλειψοειδών που περιέχονται στο K. Ο F. John (1948) έδειξε ότι υπάρχει μοναδικό ελλειψοειδές E που περιέχεται στο K και έχει τον μέγιστο δυνατό όγκο (θα λέμε ότι το E είναι το **ελλειψοειδές μέγιστου όγκου** του K) και έδειξε ότι αν η B_2^d είναι το ελλειψοειδές μέγιστου όγκου που περιέχεται στο συμμετρικό κυρτό σώμα K, τότε $K \subseteq \sqrt{d} B_2^d$.

Θεώρημα 5.2.7 (θεώρημα του John). *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$. Υποθέτουμε ότι η Ευκλείδεια μοναδιαία μπάλα B_2^d είναι το ελλειψοειδές μέγιστου όγκου που περιέχεται στο K. Τότε,*

$$K \subseteq \sqrt{d} B_2^d.$$

Απόδειξη. Υποθέτουμε ότι το συμπέρασμα δεν ισχύει. Τότε, υπάρχει x στο σύνορο του K το οποίο βρίσκεται έξω από την $\sqrt{d}B_2^d$. Αλλάζοντας συντεταγμένες αν χρειαστεί, μπορούμε να υποθέσουμε ότι $x = ae_1$, όπου $a > \sqrt{d}$. Από τη συμμετρία του K έπεται ότι,

$$K \supset W = \mathrm{co}\{B_2^d, \pm ae_1\}.$$

Για κάθε $\gamma, \delta > 0$ ορίζουμε το ελλειψοειδές

$$E_{\gamma,\delta} = \big\{x \in \mathbb{R}^d : \frac{x_1^2}{\gamma^2} + \sum_{i=2}^{d} \frac{x_i^2}{\delta^2} \leqslant 1\big\}.$$

Ισχυρισμός. Αν $\gamma > 1$ και $\gamma^2 \leqslant a^2 - a^2\delta^2 + \delta^2$, τότε $E_{\gamma,\delta} \subseteq W \subseteq K$.

[Πράγματι: λόγω της σφαιρικής συμμετρίας του $E_{\gamma,\delta}$ και του W ως προς τις $(d-1)$ τελευταίες μεταβλητές, μπορούμε να υποθέσουμε ότι $d = 2$. Τότε, το W ορίζεται από τις εφαπτόμενες από τα $(\pm a, 0)$ στον δίσκο D_2, και τον D_2. Τα σημεία επαφής των τεσσάρων εφαπτομένων με τον δίσκο είναι τα

$$\left(\pm\frac{1}{a}, \pm\frac{\sqrt{a^2-1}}{a}\right),$$

και οι εξισώσεις των τεσσάρων εφαπτομένων είναι οι

$$y = \frac{\pm a \pm x}{\sqrt{a^2-1}}.$$

Αν $\gamma > 1$, τότε η έλλειψη $E_{\gamma,\delta}$ θα περιέχεται στο W αν δεν τέμνει τις τέσσερις ευθείες, και, εξετάζοντας τη δευτεροβάθμια εξίσωση που προκύπτει, καταλήγουμε στη συνθήκη του ισχυρισμού.]

Από την άλλη πλευρά, ο όγκος του $E_{\gamma,\delta}$ ισούται με $|E_{\gamma,\delta}| = |B_2^d|\gamma\delta^{d-1}$. Αν λοιπόν $\gamma\delta^{d-1} > 1$, τότε $|E_{\gamma,\delta}| > |B_2^d|$. Με την υπόθεση ότι $a > \sqrt{d}$, θα δείξουμε ότι υπάρχουν $\gamma > 1$ και $\delta > 0$ που ικανοποιούν ταυτόχρονα τις

$$\gamma\delta^{d-1} > 1 \quad , \quad \gamma^2 = a^2 - a^2\delta^2 + \delta^2.$$

Αυτό είναι άτοπο, γιατί θα έχουμε βρεί ελλειψοειδές που περιέχεται στο K και έχει όγκο γνήσια μεγαλύτερο από τον όγκο της B_2^d.

Λύνοντας ως προς δ, έχουμε $\delta = \sqrt{\frac{a^2-\gamma^2}{a^2-1}}$, και μελετάμε τη συνάρτηση

$$f(\gamma) = \gamma\left(\frac{a^2-\gamma^2}{a^2-1}\right)^{\frac{d-1}{2}}, \quad 1 < \gamma < a.$$

Η f έχει μέγιστο στο $\gamma_0 = a/\sqrt{d}$, το οποίο ισούται με

$$f(\gamma_0) = \frac{a}{\sqrt{d}}\left(\frac{a\sqrt{d-1}}{\sqrt{d}\sqrt{a^2-1}}\right)^{d-1} > 1,$$

κάτι που μπορούμε να δείξουμε παρατηρώντας ότι η $g(x) = x^d/(x^2-1)^{(d-1)/2}$ είναι αύξουσα στο $(\sqrt{d}, +\infty)$. □

5.3 Πρώτο και δεύτερο θεώρημα του Minkowski

Πρώτο θεώρημα του Minkowski

Το *πρώτο θεώρημα του Minkowski* εξασφαλίζει την ύπαρξη μη μηδενικού σημείου με ακέραιες συντεταγμένες σε κάθε ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$ που έχει όγκο μεγαλύτερο από 2^d.

Θεώρημα 5.3.1. *Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$. Αν $|K| > 2^d$, τότε το K περιέχει τουλάχιστον ένα $u \in \mathbb{Z}^d \setminus \{0\}$.*

Το αποτέλεσμα είναι βέλτιστο: αν θεωρήσουμε τον κύβο $Q = \{x : |x_i| < 1, i = 1, \dots, d\}$, τότε $|Q| = 2^d$, αλλά $Q \cap \mathbb{Z}^d = \{0\}$. Το θεώρημα γενικεύεται άμεσα για τυχόν πλέγμα Λ στον $\mathbb{R}^d$. Αρκεί να παρατηρήσουμε ότι $\Lambda = T(\mathbb{Z}^d)$ για κάποιον $T \in GL(d)$ με $|\det T| = \det \Lambda$ και να χρησιμοποιήσουμε το θεώρημα για το συμμετρικό κυρτό σώμα $T^{-1}(K)$:

Θεώρημα 5.3.2. *Έστω Λ ένα πλέγμα στον $\mathbb{R}^d$ και έστω K ένα ανοικτό, συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$. Αν $|K| > 2^d \det \Lambda$, τότε το K περιέχει τουλάχιστον ένα $u \in \Lambda \setminus \{0\}$.*

Η απόδειξη θα βασιστεί στο λήμμα του Blichfeldt:

Θεώρημα 5.3.3. *Έστω M μετρήσιμο υποσύνολο του $\mathbb{R}^d$, με $|M| > 1$. Υπάρχουν $x \neq y$ στο M ώστε $x - y \in \mathbb{Z}^d \setminus \{0\}$.*

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 $\mathbb{Z}^d$

$$P = \{x \in \mathbb{R}^d : 0 \leqslant x_i < 1, i = 1, \dots, d\}.$$

Το σύνολο των $u \in \mathbb{Z}^d$ 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

$$\sum_{r=1}^{r_0} |M'_r| = \sum_{r=1}^{r_0} |M_r| = \sum_{r=1}^{r_0} |(u^r + P) \cap M| = \sum_{u \in \mathbb{Z}^d} |(u + P) \cap M| = |M| > 1,$$

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 $x - y = u^r - u^s \in \mathbb{Z}^d \setminus \{0\}$. □

Παρατήρηση. 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 $0 \neq x_r - y_r \in \mathbb{Z}^d$. 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 $x - y \in \mathbb{Z}^d \setminus \{0\}$.

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 $0 \neq x - y \in \mathbb{Z}^d$. 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 o, άρα $-w_2 \in K$, και κυρτό, άρα

$$x - y = \frac{w_1 + (-w_2)}{2} \in K.$$

Δηλαδή, $0 \neq x - y \in K \cap \mathbb{Z}^d$. □

Έστω K κλειστό κυρτό σώμα στον $\mathbb{R}^d$, το οποίο περιέχει το o στο εσωτερικό του. Ο **συντελεστής ασυμμετρίας** του K ως προς το o, 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 o. 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 5.3.4. *Έστω K κυρτό σώμα στον $\mathbb{R}^d$, που περιέχει το 0 στο εσωτερικό του. Αν $|K| > (1 + \sigma(K))^d$, τότε $K \cap (\mathbb{Z}^d \setminus \{0\}) \neq \emptyset$.*

Απόδειξη. Θεωρούμε το σώμα $K_1 = (1 + \sigma)^{-1}K$. Τότε, $|K_1| > 1$, άρα υπάρχουν $x, y \in K_1$ ώστε $y - x \in \mathbb{Z}^d \setminus \{0\}$. 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, $y - x \in K \cap (\mathbb{Z}^d \setminus \{0\})$. □

Διαδοχικά ελάχιστα συμμετρικού κυρτού σώματος

Έστω K ένα ανοικτό, συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$. 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 $\lambda K \cap \mathbb{Z}^d = \{0\}$. Από την άλλη πλευρά, το K περιέχει μία μπάλα με κέντρο το 0. Αν λοιπόν το λ είναι αρκετά μεγάλο, τότε το λK περιέχει d γραμμικά ανεξάρτητα διανύσματα του $\mathbb{Z}^d$. Επομένως, για κάθε $i = 1, \ldots, d$, υπάρχουν $\lambda > 0$ τέτοια ώστε το λK να περιέχει τουλάχιστον i γραμμικά ανεξάρτητα διανύσματα του $\mathbb{Z}^d$. Ορίζουμε

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^d) \geqslant i\}, \quad i = 1, \ldots, d,$$

όπου $\dim(\lambda K \cap \mathbb{Z}^d)$ είναι η διάσταση του υποχώρου που παράγεται από τα ακέραια σημεία του λK.

Λήμμα 5.3.5. *Ισχύει*

$$A_i := \{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^d) \geqslant i\} = (\lambda_i, \infty).$$

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 $\mathbb{Z}^d$). Είναι φανερό ότι

$$0 < \lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_d.$$

Μπορεί να συμβεί κάποια από τα λ_i να είναι ίσα. Για παράδειγμα, αν $K = \{x : |x_i| < 1\}$, τότε $\lambda_1 = \ldots = \lambda_d = 1$.

Πρόταση 5.3.6. *Έστω K ανοικτό, συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$. Υπάρχουν γραμμικώς ανεξάρτητα διανύσματα $u_1, \ldots, u_d \in \mathbb{Z}^d$ που ικανοποιούν τα εξής:*

(i) $u_i \notin \langle u_1, \ldots, u_{i-1}\rangle$, $i = 1, \ldots, d$.

(ii) $u_i \notin \lambda_i K$, $i = 1, \ldots, d$.

(iii) $u_i \in \lambda_i \overline{K}$, $i = 1, \ldots, d$.

Απόδειξη. Ορίζουμε επαγωγικά $u_1, \ldots, u_d \in \mathbb{Z}^d$ 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 λήμμα μας εξασφαλίζει ότι

$$\dim(\lambda_{j+1} K \cap \mathbb{Z}^d) = j.$$

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 $\lambda K \cap \mathbb{Z}^d = \lambda_{j+1}\overline{K} \cap \mathbb{Z}^d$. Όμως $\lambda > \lambda_{j+1}$, άρα $\dim(\lambda K \cap \mathbb{Z}^d) \geqslant j+1$. Έπεται ότι

$$\dim(\lambda_{j+1}\overline{K} \cap \mathbb{Z}^d) = k > j.$$

Υπάρχουν λοιπόν γραμμικά ανεξάρτητα $u_{j+1}, \ldots, u_k$ στο σύνορο του $\lambda_{j+1} K$, τα οποία δεν ανήκουν στον υπόχωρο $\langle \lambda_{j+1} K \cap \mathbb{Z}^d\rangle$. Τα $u_1, \ldots, u_k$ ικανοποιούν τα (1)-(3), και από την κατασκευή,

$$\lambda_{j+1} = \ldots = \lambda_k.$$

Συνεχίζουμε με τον ίδιο τρόπο, ορίζοντας τα u_i κατά ομάδες. □

Παρατήρηση. Τα λ_i ορίζονται μονοσήμαντα από το K, ενώ το $\{u_1, \ldots, u_d\}$ μπορεί να μην επιλέγεται κατά μοναδικό τρόπο. Τα διανύσματα u_i της Πρότασης ονομάζονται *ελαχιστικά διανύσματα* του K (ως προς το πλέγμα $\mathbb{Z}^d$).

Δεύτερο θεώρημα του Minkowski

Σύμφωνα με το πρώτο θεώρημα του Minkowski, αφού $\lambda_1 K \cap \mathbb{Z}^d = \{0\}$, το $\lambda_1 K$ πρέπει να έχει όγκο το πολύ ίσο με 2^d. Με άλλα λόγια,

$$\lambda_1^d |K| \leqslant 2^d.$$

Παίρνοντας υπ' όψιν του όλα τα διαδοχικά ελάχιστα $\lambda_1, \ldots, \lambda_d$ του K, ο Minkowski απέδειξε κάτι ισχυρότερο:

Θεώρημα 5.3.7 (δεύτερο θεώρημα του Minkowski)**.** *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^s$. Τότε,*

$$\lambda_1\lambda_2\dots\lambda_d|K| \leqslant 2^d.$$

Άμεση γενίκευση του Θεωρήματος για τυχόν πλέγμα Λ στον $\mathbb{R}^d$ είναι το εξής:

Θεώρημα 5.3.8. *Έστω Λ πλέγμα στον $\mathbb{R}^d$, και K συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$. Τότε,*

$$\lambda_1\lambda_2\dots\lambda_d|K| \leqslant 2^d \det\Lambda,$$

όπου

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

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 $\mathbb{R}^d$, υποθέτουμε ότι $u_1,\dots,u_d$ είναι μια επιλογή ελαχιστικών διανυσμάτων του, και ότι

$$\lambda_1\lambda_2\dots\lambda_d|K| > 2^d.$$

Θεωρούμε τον γραμμικό μετασχηματισμό T που ορίζεται από τις $T(u_i) = \lambda_i u_i$, $i = 1,\dots,d$. Τότε, το $W = T(K)$ έχει όγκο $|W| = \lambda_1\dots\lambda_d|K| > 2^d$, οπότε το πρώτο θεώρημα του Minkowski μας δίνει $a_1,\dots,a_d \in \mathbb{R}$ ώστε

$$0 \neq w = a_1\lambda_1u_1 + \dots + a_d\lambda_du_d \in W \cap \mathbb{Z}^d.$$

Αφού $w \neq 0$, υπάρχει $k \leqslant d$ με την ιδιότητα

$$a_k \neq 0, \quad a_{k+1} = \dots = a_d = 0.$$

Γράφουμε το w στην εξής μορφή:

$$w = \lambda_1(a_1u_1 + \dots + a_ku_k) + (\lambda_2 - \lambda_1)(a_2u_2 + \dots + a_ku_k) + \dots + (\lambda_k - \lambda_{k-1})a_ku_k.$$

Αφού $w = T(a_1u_1 + \dots + a_ku_k)$, γνωρίζουμε ότι $a_1u_1 + \dots + a_ku_k \in K$. Ας υποθέσουμε πρός στιγμήν ότι τα διανύσματα $a_2u_2 + \dots + a_ku_k, \dots, a_ku_k$ είναι όλα μέσα στο K. Τότε, από την κυρτότητα του K και την $(*)$, συμπεραίνουμε ότι

$$w \in \lambda_1K + (\lambda_2 - \lambda_1)K + \dots + (\lambda_k - \lambda_{k-1})K = \lambda_kK.$$

Αυτό όμως είναι άτοπο. Θα είχαμε

$$w \in \lambda_kK \setminus \langle u_1,\dots,u_{k-1}\rangle,$$

δηλαδή το w θα ήταν ακέραιο σημείο του λ_kK γραμμικά ανεξάρτητο προς 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 $u_1,\dots,u_d$ του K, και γράφουμε το τυχόν στοιχείο του K στη μορφή $a = a_1u_1 + \dots + a_du_d$.

Για κάθε $a = a_1u_1 + \ldots + a_du_d \in \mathbb{R}^d$ και $k = 1, \ldots, d-1$, ορίζουμε

$$L(a_{k+1}, \ldots, a_d) = \{x = \sum_{i=1}^{d} x_i u_i \in \mathbb{R}^d : x_{k+1} = a_{k+1}, \ldots, x_d = a_d\},$$

τον συσχετισμένο υπόχωρο των σημείων που συμπίπτουν με το a στις συντεταγμένες $x_{k+1}, \ldots, x_d$ (ως προς τη βάση $\{u_1, \ldots, u_d\}$). Ορίζουμε $b(a_{k+1}, \ldots, a_d)$ το κέντρο βάρους του $K \cap L(a_{k+1}, \ldots, a_d)$. [Προφανώς, $b(a_1, \ldots, a_d) = a$.] Δηλαδή, η i συντεταγμένη ($i \leqslant k$) του $b(a_{k+1}, \ldots, a_d)$ δίνεται από το

$$\int_{K \cap L(a_{k+1}, \ldots, a_d)} x_i dx_k \ldots dx_1.$$

Το $b(a_{k+1}, \ldots, a_d)$ ανήκει στο $K \cap L(a_{k+1}, \ldots, a_d)$, και όλες οι απεικονίσεις $a \mapsto b(a_{k+1}, \ldots, a_d)$ είναι παραγωγίσιμες ως προς a_i στο K.

Λήμμα 5.3.9. *Ο μετασχηματισμός $T : K \to K$ που ορίζεται από την*

$$a = (a_1, \ldots, a_d) \mapsto \lambda_1 b(a_1, \ldots, a_d) + (\lambda_2 - \lambda_1) b(a_2, \ldots, a_d) + \ldots + (\lambda_d - \lambda_{d-1}) b(a_d)$$

είναι ένα προς ένα.

Απόδειξη. Το $b(a_{k+1}, \ldots, a_d)$ γράφεται στη μορφή

$$b(a_{k+1}, \ldots, a_d) = \sum_{j=1}^{k} c_j(a_{k+1}, \ldots, a_d) u_j + \sum_{j=k+1}^{d} a_j u_j,$$

όπου c_j συναρτήσεις που εξαρτώνται μόνο από τα $a_{k+1}, \ldots, a_d$, $j = 1, \ldots, k$.

Έστω $a = \sum_{k=1}^{n} d a_k u_k \in K$. Τότε, $T(a) = \sum_{k=1}^{d} s_k u_k$, όπου

$$(*) \qquad s_k = \lambda_k a_k + \sum_{j=k}^{d-1} (\lambda_{j+1} - \lambda_j) c_j(a_{k+1}, \ldots, a_d) = \lambda_k a_k + h(a_{k+1}, \ldots, a_d).$$

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 $k = d$, η $(*)$ δίνει $s_d = \lambda_d a_d$, άρα $a_d = s_d/\lambda_d$. Τότε,

$$s_{d-1} = \lambda_{d-1} a_{d-1} + h(s_d/\lambda_d),$$

απ' όπου προσδιορίζεται το a_{d-1}, και πηγαίνοντας προς τα πίσω προσδιορίζουμε μονοσήμαντα τα $a_{d-2}, \ldots, a_1$ για τα οποία $T(a) = \sum_{k=1}^{d} s_k u_k$. □

Λήμμα 5.3.10. *Ο μετασχηματισμός T «πολλαπλασιάζει» τον όγκο του K με τον παράγοντα $\lambda_1 \ldots \lambda_d$:*

$$|T(K)| = \lambda_1 \ldots \lambda_d |K|.$$

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 $\lambda_1 \ldots \lambda_d$ στο K. Αυτό είναι συνέπεια του ορισμού του T. Η Ιακωβιανή του T είναι άνω τριγωνικός πίνακας (το s_k εξαρτάται μόνο από τα $a_k, \ldots, a_d$), και

$$\frac{\partial s_k(a_k, \ldots, a_d)}{\partial a_k} = \lambda_k, \quad k = 1, \ldots, d,$$

από την $(*)$. □

Ας υποθέσουμε τώρα ότι $\lambda_1 \dots \lambda_d |K| > 2^d$. Από το Λήμμα 4.2.2 και το θεώρημα αντίστροφης απεικόνισης, το $T(K)$ είναι ανοικτό και φραγμένο, και $|T(K)| > 2^d$, οπότε, εφαρμόζοντας το Λήμμα του Blichfeldt για το $\frac{T(K)}{2}$, βρίσκουμε $y^1 \neq y^2 \in \frac{T(K)}{2}$ ώστε

$$\frac{y^1 - y^2}{2} \in \mathbb{Z}^d \setminus \{0\}.$$

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

$$a^1 = \sum_{j=1}^{d} a_j^1 u_j, \quad a^2 = \sum_{j=1}^{d} a_j^2 u_j.$$

Αφού $a^1 \neq a^2$, υπάρχει $k \leqslant d$ ώστε $a_k^1 \neq a_k^2$, και $a_j^1 = a_j^2$, $j = k+1, \dots, d$. Τότε,

$$\begin{aligned}\frac{y^1 - y^2}{2} &= \lambda_1 \frac{1}{2}(b(a_1^1, \dots, a_d^1) - b(a_1^2, \dots, a_d^2)) + \dots \\ &\quad + (\lambda_k - \lambda_{k-1}) \frac{1}{2}(b(a_k^1, \dots, a_d^1) - b(a_k^2, \dots, a_d^2)).\end{aligned}$$

Από την κυρτότητα και τη συμμετρία του K, και από το γεγονός ότι όλες οι b παίρνουν τιμές στο K, συμπεραίνουμε ότι

$$\frac{y^1 - y^2}{2} \in \lambda_1 K + \dots + (\lambda_k - \lambda_{k-1})K = \lambda_k K.$$

Δηλαδή,

$$\frac{y^1 - y^2}{2} \in \lambda_k K \cap (\mathbb{Z}^d \setminus \{0\}).$$

Όμως, η k-στή συντεταγμένη του $(y^1 - y^2)/2$ (ως προς τη βάση $\{u_1, \dots, u_d\}$) είναι

$$\frac{1}{2}\left(\lambda_k a_k^1 + h(a_{k+1}^1, \dots, a_d^1) - \lambda_k a_k^2 - h(a_{k+1}^2, \dots, a_d^2)\right) = \frac{1}{2}\lambda_k (a_k^1 - a_k^2) \neq 0,$$

δηλαδή το $(y^1 - y^2)/2$ είναι γραμμικώς ανεξάρτητο από τα $u_1, \dots, u_{k-1}$. Αυτό είναι άτοπο, αφού το $\lambda_k K$ δεν μπορεί να περιέχει k γραμμικά ανεξάρτητα ακέραια σημεία. □

5.4 Πρόοδοι

Λήμμα 5.4.1. *Έστω $P = a + [0, N] \cdot v$ πρόοδος τάξης d στην G. Για κάθε $b \in G$ και για κάθε $m > n$ στο $\mathbb{Z}$, η πρόοδος $P_1 = b + [nN, mN] \cdot v$ καλύπτεται από $(m-n)^d$ μεταφορές της P.*

Ειδικότερα, αν $n, m \geqslant 0$ και $(n, m) \neq (0, 0)$ τότε το $nP - mP$ καλύπτεται από $(n+m)^d$ μεταφορές της P και

$$|nP - mP| \leqslant (n+m)^d |P|.$$

Το $nP - mP$ είναι επίσης πρόοδος τάξης d και έχει όγκο $\mathrm{vol}(nP - mP) \leqslant (n+m)^d \mathrm{vol}(P)$.

Απόδειξη. □

Λήμμα 5.4.2. *Έστω P πρόοδος τάξης d και έστω $P + w_1, \dots, P + w_k$ μεταφορές της P. Υπάρχει πρόοδος P_1 τάξης $d + k - 1$ και όγκου $\mathrm{vol}(P_1) = 2^{k-1}\mathrm{vol}(P)$ ώστε*

$$(P + w_1) \cup \dots \cup (P + w_k) \subseteq P_1.$$

Απόδειξη. □

5.5 Κυρτά σώματα και πλέγματα

Δείχνουμε πρώτα δύο βασικά λήμματα για αριθμούς κάλυψης.

Λήμμα 5.5.1 (Ruzsa). *Έστω A, B φραγμένα, όχι αναγκαστικά κυρτά, υποσύνολα του $\mathbb{R}^d$ με θετικό μέτρο. Τότε,*

$$N(B, A-A) \leqslant \min\left\{\frac{|A+B|}{|A|}, \frac{|A-B|}{|A|}\right\}.$$

Απόδειξη. □

Λήμμα 5.5.2. *Έστω A κυρτό σώμα στον $\mathbb{R}^d$ και έστω $\lambda, \mu > 0$. Τότε,*

$$N(\lambda \cdot A, A-A) \leqslant (\lambda+1)^d$$

και

$$N(\lambda \cdot A - \mu \cdot A, A-A) \leqslant (2\max\{\lambda,\mu\}+1)^d.$$

Αν το A είναι συμμετρικό, τότε

$$N(\lambda \cdot A, A) \leqslant (2\lambda+1)^d.$$

Απόδειξη. □

Λήμμα 5.5.3. (i) *Έστω Λ πλέγμα στον $\mathbb{R}^d$. Για κάθε φραγμένο υποσύνολο A του $\mathbb{R}^d$ και για κάθε πεπερασμένο σύνολο $P \subset \mathbb{R}^d$ ισχύει*

$$|A \cap (\Lambda + P)| \leqslant |(A-A) \cap (\Lambda + P - P)|.$$

(ii) *Αν B είναι συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$, τότε*

$$N((k \cdot B) \cap \Lambda, B \cap \Lambda) \leqslant (4k+1)^d$$

για κάθε $k \in \mathbb{N}$.

(iii) *Αν Λ_1 είναι υποπλέγμα του Λ, τότε*

$$|B \cap \Lambda_1| \leqslant |B \cap \Lambda| \leqslant 9^d |\Lambda : \Lambda_1|\, |B \cap \Lambda_1|.$$

Απόδειξη. □

Λήμμα 5.5.4. *Έστω B συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$ και έστω Λ πλέγμα στον $\mathbb{R}^d$. Υπάρχει συμμετρικό κυρτό σώμα $B_1 \subseteq B$ ώστε*

$$B_1 \cap \Lambda = \{0\}$$

και

$$B \subseteq Cd^{3/2} \cdot B_1 + (Cd^{3/2} \cdot B) \cap \Lambda.$$

Επιπλέον,

$$\frac{|B|}{(c_1 d)^{5d/2} |B \cap \Lambda|} \leqslant |B_1| \leqslant c_2^d \frac{|B|}{|B \cap \Lambda|}.$$

Απόδειξη. □

Λήμμα 5.5.5. *Έστω B συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$ και έστω Λ πλέγμα στον $\mathbb{R}^d$. Υπάρχει γνήσια πρόοδος P η οποία περιέχεται στο $B \cap \Lambda$, έχει τάξη το πολύ ίση με d και πληθάριθμο*

$$|P| \geqslant \frac{1}{(cd)^{7d/2}}|B \cap \Lambda|.$$

Απόδειξη. □

Θεώρημα 5.5.6 (Mahler)**.** *Έστω Λ πλέγμα πλήρους διάστασης στον $\mathbb{R}^d$ και έστω B ένα συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$ με διαδοχικά ελάχιστα $0 < \lambda_1 \leqslant \cdots \leqslant \lambda_d$ με αντίστοιχη βάση τα $v_1, \ldots, v_d$. Τότε, υπάρχει βάση $w_1, \ldots, w_d$ του Λ ώστε: κάθε w_i ανήκει στην κλειστή θήκη του $\lambda_i \cdot B$ και, για κάθε $i = 2, \ldots, d$, το w_i ανήκει στην κλειστή θήκη του $\frac{i\lambda_i}{2} \cdot B$. Επιπλέον, αν $V_i = \operatorname{span}\{v_1, \ldots, v_i\}$ τότε το $\{w_1, \ldots, w_i\}$ είναι βάση του $\Lambda \cap V_i$.*

Απόδειξη. □

Πόρισμα 5.5.7. *Έστω Λ πλέγμα πλήρους διάστασης στον $\mathbb{R}^d$. Υπάρχει βάση $\{w_1, \ldots, w_d\}$ του Λ ώστε*

$$|Q_\Lambda| = \|\det(w_1, \ldots, w_d)| \geqslant \frac{1}{(cd)^{3d/2}}\|w_1\|_2 \cdots \|w_d\|_2.$$

Απόδειξη. □

Θεώρημα 5.5.8 (διακριτό θεώρημα John)**.** *Έστω B συμμετρικό κυρτό σώμα στον $\mathbb{R}^d$ και έστω Λ πλέγμα τάξης r στον $\mathbb{R}^d$. Υπάρχουν γραμμικά ανεξάρτητα διανύσματα $w_1, \ldots, w_r \in \Lambda$ και $N_1, \ldots, N_r \in \mathbb{N}$ ώστε*

$$(r^{-2r} \cdot B) \cap \Lambda \subseteq (-N, N) \cdot w \subseteq B \cap \Lambda \subseteq (-r^{2r}N, r^{2r}N) \cdot w,$$

όπου $w = (w_1, \ldots, w_r)$ και $N = (N_1, \ldots, N_r)$.

Απόδειξη. □

5.6 Πρόοδοι και γνήσιες πρόοδοι

Θεώρημα 5.6.1. *Έστω P πρόοδος τάξης d στην προσθετική ομάδα G. Υπάρχει γνήσια πρόοδος $P_1 \subseteq P$ η οποία έχει τάξη το πολύ ίση με d και πληθάριθμο*

$$|P_1| \geqslant \frac{1}{(cd)^{5d}}|P|.$$

Απόδειξη. □

Θεώρημα 5.6.2. *Έστω P πρόοδος τάξης d στην προσθετική ομάδα G. Υπάρχει γνήσια πρόοδος $P_2 \supseteq P$ η οποία έχει τάξη το πολύ ίση με d και πληθάριθμο*

$$|P_2| \leqslant d^{cd^3}|P|.$$

Απόδειξη. □

ΚΕΦΑΛΑΙΟ 6

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 6.0.3 (λόγος μεγέθυνσης)**.** Έστω $G = (A, B, E)$ ένα κατευθυνόμενο διμερές γράφημα. Ο *λόγος μεγέθυνσης* $\|G\|$ του G είναι η ποσότητα

$$\|G\| = \min\left\{\frac{|G(X)|}{|X|} : X \subseteq A, G \neq \emptyset\right\}. \tag{6.0.1}$$

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 6.0.4 (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 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.

Παράδειγμα 6.0.5. 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,

$$\|G_{A,B}\| = \min\left\{\frac{|X + A|}{|X|} : X \subseteq A,\, X \neq \emptyset\right\} \leqslant \frac{|A + B|}{|A|}. \tag{6.0.2}$$

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

$$G_{A+B,C} \circ G_{A,B} = G_{A,B+C}. \tag{6.0.3}$$

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

Θεώρημα 6.0.6 (θεώρημα Plünnecke)**.** *Έστω $(G_1, \dots, G_k)$ ένα γράφημα Plünnecke τάξης k. Τότε, η ακολουθία των λόγων μεγέθυνσης $\|G_i \circ \cdots \circ G_1\|^{1/i}$, $i = 1, \dots, k$, είναι φθίνουσα. Ειδικότερα,*

$$\|G_k \circ \cdots \circ G_1\| \leqslant \|G_1\|^k. \tag{6.0.4}$$

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

Θεώρημα 6.0.7 (ανισότητα Plünnecke)**.** *Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G που ικανοποιούν την $|A+B| \leqslant K|A|$. Τότε, για κάθε $k \in \mathbb{N}$ υπάρχει $X \subseteq A$ ώστε*

$$|X + kB| \leqslant K^k |X|. \tag{6.0.5}$$

Ειδικότερα,

$$|kB| \leqslant K^k |A|. \tag{6.0.6}$$

Απόδειξη. Θεωρούμε το γράφημα Plünnecke $(G_{A,B}, G_{A+B,B}, \dots, G_{A+(k-1)B,B})$. Από την υπόθεση έχουμε

$$\|G_{A,B}\| \leqslant \frac{|A+B|}{|A|} \leqslant K. \tag{6.0.7}$$

Τότε, το θεώρημα 1.5.4 μας εξασφαλίζει ότι

$$\|G_{A+(k-1)B,B} \circ \cdots \circ G_{A+B,B} \circ G_{A,B}\| \leqslant K^k. \tag{6.0.8}$$

Αυτό σημαίνει ότι υπάρχει $X \subseteq A$ ώστε

$$|(G_{A+(k-1)B,B} \circ \cdots \circ G_{A+B,B} \circ G_{A,B})(X)| \leqslant K^k |X|. \tag{6.0.9}$$

Όμως, $(G_{A+(k-1)B,B} \circ \cdots \circ G_{A+B,B} \circ G_{A,B})(X) = X + kB$, συνεπώς $|X + kB| \leqslant K^k |X|$. □

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

Θεώρημα 6.0.8 (θεώρημα Plünnecke–Ruzsa)**.** *Έστω A και B πεπερασμένα υποσύνολα της αβελιανής ομάδας G ώστε $|A+B| \leqslant K|A|$. Τότε,*

$$|nB - mB| \leqslant K^{n+m} |A| \tag{6.0.10}$$

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

Απόδειξη. Από το θεώρημα 1.5.5 υπάρχει $X \subseteq A$ ώστε

$$|X + nB| \leqslant K^n |X|.$$

Πάλι από το θεώρημα 1.5.5, υπάρχει $Y \subseteq X$ ώστε

$$|Y + mB| \leqslant K^m |Y|.$$

Εφαρμόζοντας την τριγωνική ανισότητα $|U|\,|V - W| \leqslant |U + V|\,|U + W|$ για τα Y, nB και mB παίρνουμε

$$|Y|\,|nB - mB| \leqslant |Y + nB|\,|Y + mB| \leqslant |X + nB|\,|Y + mB| \leqslant K^n |X|\,K^m |Y|.$$

Έπεται ότι

$$|nB - mB| \leqslant K^{n+m} |X| \leqslant K^{n+m} |A|.$$

□

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

$$\|G_k \circ \cdots \circ G_1\|^{1/k} \leqslant \|G_i \circ \cdots \circ G_1\|^{1/i}. \tag{6.0.11}$$

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

$$\|G_{i+1} \circ \cdots \circ G_1\|^{1/(i+1)} \leqslant \|G_i \circ \cdots \circ G_1\|^{1/i}. \tag{6.0.12}$$

Σαν πρώτο βήμα για την απόδειξη της (1.5.11) θα δείξουμε πρώτα την ακόλουθη «κανονικοποιημένη» έκδοση της ανισότητας:

Θεώρημα 6.0.9 (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,*

$$\|G_i \circ \cdots \circ G_1\| \geqslant 1, \quad 1 \leqslant i < k. \tag{6.0.13}$$

Για την απόδειξη του θεωρήματος 1.5.7 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 (η απόδειξη θα δοθεί στο τέλος της παραγράφου).

Θεώρημα 6.0.10 (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 6.0.11. *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 αποφεύγε 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 6.0.12. *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

$$\|G_k \circ \cdots \circ G_1\| \leqslant \frac{|C_k|}{|X|}. \tag{6.0.14}$$

Από την άλλη πλευρά, $|C_0| + |C_k| = N$ και $|X| = |A_0| - |C_0|$. Τότε,

$$\frac{N - |C_0|}{|A_0| - |C_0|} \geqslant \|G_k \circ \cdots \circ G_1\| \geqslant 1, \tag{6.0.15}$$

άρα $N \geqslant |A_0|$. □

Απόδειξη του θεωρήματος 1.5.7. 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 1.5.7. Εδώ χρησιμοποιείται το τέχνασμα της «ύψωσης σε δύναμη»: χρησιμοποιώντας την κανονικοποιημένη ανισότητα του θεωρήματος 1.5.7 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 6.0.13. *Ισχύουν οι ισότητες*

$$\|G \oplus H\| = \|G\| \, \|H\| \tag{6.0.16}$$

και

$$(G_k \circ \cdots \circ G_1) \oplus (H_k \circ \cdots \circ H_1) = (G_k \oplus H_k) \circ \cdots \circ (G_1 \oplus H_1). \tag{6.0.17}$$

Απόδειξη. Ας υποθέσουμε ότι $G : A \to B$ και $H : C \to D$. Θεωρούμε $X \subseteq A$ και $Y \subseteq C$ ώστε

$$\|G\| = \frac{|G(X)|}{|X|} \text{ και } \|H\| = \frac{|H(Y)|}{|Y|}. \tag{6.0.18}$$

Τότε, $X \times Y \subseteq A \times C$ και $(G \oplus H)(X \times Y) \subseteq G(X) \times H(Y)$. Συνεπώς,

$$\|G\| \, \|H\| = \frac{|G(X)| \, |H(Y)|}{|X| \, |Y|} \geqslant \frac{|(G \oplus H)(X \times Y)|}{|X \times Y|} \geqslant \|G \oplus H\|. \tag{6.0.19}$$

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

$$Z = \{(a, d) : \text{ υπάρχει } b \in D \text{ ώστε } (a, b) \in U \text{ και } b \mapsto_H d\} \tag{6.0.20}$$

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

$$|Z| = \sum |H(Y_a)| \geqslant \|H\| \sum |Y_a| = \|H\|\,|U|. \tag{6.0.21}$$

Από την άλλη πλευρά, $(G \oplus H)(U) = \bigcup(G(X_d) \times \{d\})$, άρα

$$|(G \oplus H)(U)| = \sum |G(X_d)| \geqslant \|G\| \sum |X_d| = \|G\|\,|Z|. \tag{6.0.22}$$

Συνδυάζοντας τις δύο ανισότητες βλέπουμε ότι

$$|(G \oplus H)(U)| \geqslant \|G\|\,\|H\|\,|U|, \tag{6.0.23}$$

απ' όπου έπεται ότι $\|G \oplus H\| \geqslant \|G\|\,\|H\|$.

Ο δεύτερος ισχυρισμός προκύπτει απλά από τους ορισμούς. □

Λήμμα 6.0.14. *Έστω $k \geqslant 2$ και $(G_1, \dots, G_k)$ ένα γράφημα Plünnecke τάξης k. Τότε, για κάθε $m \geqslant 1$,*

$$\|G_k \circ \cdots \circ G_1\|^{1/k} \leqslant C_{i,k}\,\|G_i \circ \cdots \circ G_1\|^{1/i} \tag{6.0.24}$$

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

$$\|G_k \circ \cdots \circ G_1\|^{1/k} \geqslant \frac{k}{N}. \tag{6.0.25}$$

Τότε $N \geqslant k \geqslant 2$ και από την επιλογή του N έπεται ότι

$$\|G_k \circ \cdots \circ G_1\|^{1/k} < \frac{k}{N-1} \leqslant \frac{2k}{n}. \tag{6.0.26}$$

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

$$(H_1, \dots, H_k) = (G_{0,E}, G_{E,E}, G_{2E,E}, \dots, G_{(k-1)E,E}) \tag{6.0.27}$$

με το συμβολισμό του Παραδείγματος 1.5.3. 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

$$\frac{N^i}{i^i} < \frac{N^i}{i!} \leqslant \frac{(N+i-1)!}{(N-1)!i!} \leqslant N^i, \tag{6.0.28}$$

συμπεραίνουμε ότι

$$\frac{1}{i}N \leqslant \|H_i \circ \cdots \circ H_1\|^{1/i} \leqslant N. \tag{6.0.29}$$

Θεωρούμε το γράφημα $G' = G \oplus H$. Χρησιμοποιώντας το Λήμμα 1.5.11, παίρνουμε

$$\|G'\|^{1/k} = \|G\|^{1/k}\|H\|^{1/k} \geqslant \frac{k}{N}\frac{N}{k} = 1, \tag{6.0.30}$$

δηλαδή το G' ικανοποιεί την υπόθεση του θεωρήματος 1.5.7. Εφαρμόζοντας το θεώρημα για το G' βλέπουμε ότι, για κάθε $1 \leqslant\leqslant k$,

$$\|G'_1 \circ \cdots \circ G'_1\|^{1/i} = \|G_i \circ \cdots \circ G_1\|^{1/i}\|H_i \circ \cdots \circ H_1\|^{1/i} \geqslant 1. \tag{6.0.31}$$

Αφού $\|H_i \circ \cdots \circ H_1\|^{1/i} \leqslant N$, έπεται ότι

$$\|G_i \circ \cdots \circ G_1\|^{1/i} \geqslant \frac{1}{N} \geqslant \frac{1}{2k}\|G_k \circ \cdots \circ G_1\|^{1/k}, \tag{6.0.32}$$

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

$$\frac{1}{i}\frac{1}{N} \leqslant \|H_i^* \circ \cdots \circ H_1^*\|^{1/i} \leqslant \frac{1}{N}. \tag{6.0.33}$$

Τα υπόλοιπα βήματα της απόδειξης μένουν ως έχουν. □

Απόδειξη του θεωρήματος 1.5.4. Εφαρμόζουμε το θεώρημα 1.5.7 για το γράφημα $G^{\oplus m}$, $m \in \mathbb{N}$. Χρησμοποιώντας το Λήμμα 1.5.11 και το Λήμμα 1.5.12 βλέπουμε ότι

$$\|G_k \circ \cdots \circ G_1\|^{m/k} \leqslant C_{i,k}\|G_i \circ \cdots \circ G_1\|^{m/i} \tag{6.0.34}$$

για κάθε $m \in \mathbb{N}$. Παίρνοντας m-οστές ρίζες και αφήνοντας το $m \to \infty$ συμπεραίνουμε ότι $\|G_k \circ \cdots \circ G_1\|^{1/k} \leqslant \|G_i \circ \cdots \circ G_1\|^{1/i}$. □

ΚΕΦΑΛΑΙΟ 7

Το θεώρημα του Freiman

7.1 Πολυδιάστατες αριθμητικές πρόοδοι

Θεώρημα 7.1.1 (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*

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

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

Θεώρημα 7.1.2. *Έστω G μια αβελιανή ομάδα και έστω Q και Q' πολυδιάστατες αριθμητικές πρόοδοι στην Gδιαστάσεων n και n' και μήκους 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. □

7.2 Ισομορφισμοί Freiman

Θεώρημα 7.2.1. *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. □

Πόρισμα 7.2.2. *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. □

Πόρισμα 7.2.3. *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. □

Θεώρημα 7.2.4. *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. □

Θεώρημα 7.2.5. *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, πεερασμένα σύνολα που είναι Freiman ισομορφικά, τάξης h'. Τότε, τα σύνολα διαφορών $kA - \ell A$ και $kB - \ell B$ είναι Freiman ισομορφικά, τάξης h.*

Απόδειξη. □

7.3 Η μέθοδος του Bogolyubov

Θεώρημα 7.3.1 (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 $r_1, r_2, \ldots, r_n \in \mathbb{Z}/m\mathbb{Z}$ τέτοιες ώστε $r_1 = 0$ και*

$$B(r_1, \ldots, r_n; 1/4) \subseteq 2A - 2A.$$

Απόδειξη. □

Θεώρημα 7.3.2. *Έστω $m \geqslant 2$, και έστω $R = \{r_1, \ldots, r_n\}$ ένα σύνολο κλάσεων ισοτιμίας $\bmod\ m$. Αν $(r_1, \ldots, r_n, m) = 1$, τότε υπάρχει γνήσια n-διάστατη αριθμητική πρόοδος στο $\mathbb{Z}/m\mathbb{Z}$ η οποία περιέχεται στην Bohr περιοχή $B(r_1, \ldots, r_n; 1/4)$ και έχει πληθάριθμο*

$$|Q| > \frac{m}{(4n)^n}.$$

Απόδειξη. □

Θεώρημα 7.3.3. *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. □

7.4 Το θεώρημα του Ruzsa

Θεώρημα 7.4.1 (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. □

Θεώρημα 7.4.2. *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 εριέχεται σε μια 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. □

ΚΕΦΑΛΑΙΟ 8

Εφαρμογές του θεωρήματος του Freiman