ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικό και Καποδιστριακό
Πανεπιστήμιο Αθηνών

Κυρτή Ανάλυση

Ενότητα: Γεωμετρία των αριθμών

Απόστολος Γιαννόπουλος

Τμήμα Μαθηματικών

΄Αδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αθηνών» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Περιεχόμενα ενότητας

3 Γεωμετρία των αριθμών

3.1 Το θεώρημα του Minkowski

Πολλά από τα προβλήματα της γεωμετρίας των αριθμών διατυπώνονται στην εξής μορφή: Δίνονται μία συνάρτηση $F : \mathbb{R}^n \to \mathbb{R}$ με $F(0,\dots,0) = 0$ και ένας θετικός πραγματικός αριθμός λ. Το ζητούμενο είναι να βρεθεί μη τετριμμένη n-άδα ακεραίων $a_1,\dots,a_n$ που ικανοποιούν την

$$|F(a_1,\dots,a_n)| \leq \lambda. \tag{3.1.1}$$

Θεωρούμε την τυχούσα n-άδα $x = (x_1,\dots,x_n) \in \mathbb{R}^n$ σαν σημείο του Ευκλείδειου χώρου $\mathbb{R}^n$ και συμβολίζουμε με K το σύνολο όλων των $x \in \mathbb{R}^n$ που ικανοποιούν την

$$|F(x)| = |F(x_1,\dots,x_n)| \leq \lambda. \tag{3.1.2}$$

Τότε, το αρχικό μας πρόβλημα διατυπώνεται ισοδύναμα ως εξής: Κάτω από ποιές προϋποθέσεις το σύνολο K περιέχει σημείο $u \in \mathbb{Z}^n \setminus \{0\}$; Υπάρχουν δύο σημαντικές ιδέες πίσω από αυτή τη μετάφραση του προβλήματος. Πρώτον, παίρνουμε υπ' όψιν μας τις τιμές της F σε κάθε $x \in \mathbb{R}^n$, και όχι μόνο τις τιμές της στα $u \in \mathbb{Z}^n$. Αυτό μας δίνει τη δυνατότητα να χρησιμοποιήσουμε αναλυτικές μεθόδους για την αντιμετώπιση του προβλήματος. Δεύτερον, η ερμηνεία που δίνουμε στο πρόβλημα είναι γεωμετρική, κάτι που ευνοεί την εισαγωγή νέων εννοιών και μεθόδων οι οποίες βασίζονται στη γεωμετρική μας διαίσθηση.

Γεωμετρικές μέθοδοι αυτού του τύπου είχαν ήδη χρησιμοποιηθεί από τον Gauss και τον Dirichlet, οι οποίοι εργάζονταν σε προβλήματα σχετικά με τις θετικά ορισμένες τετραγωνικές μορφές. Πρώτος όμως ο Minkowski ανέπτυξε μία συστηματική θεωρία, απέδειξε ένα γενικό θεώρημα για n-διάστατα κυρτά σώματα K, και το εφάρμοσε σε μεγάλο πλήθος σημαντικών προβλημάτων. Η νέα θεωρία ονομάστηκε «γεωμετρία των αριθμών» από τον ίδιο τον Minkowski.

Ο Hermite (1850) απέδειξε ότι, αν F είναι μία θετικά ορισμένη τετραγωνική μορφή n μεταβλητών, τότε η (3.1.1) έχει μη τετριμμένη ακέραια λύση αν το λ ξεπερνάει μία τιμή που εξαρτάται μόνο από το n και από τη διακρίνουσα της F. Η φύση της απόδειξής του ήταν αριθμητική. Ο Minkowski μετέφρασε το αποτέλεσμα του Hermite σε ένα θεώρημα για ελλειψοειδή, και έδωσε μία νέα γεωμετρική απόδειξή του. Στη συνέχεια παρατήρησε ότι, οι μόνες ιδιότητες του ελλειψοειδούς που απαιτούνταν για την απόδειξη, ήταν η κυρτότητα και η συμμετρία του ως προς το 0. Κατέληξε έτσι στο εξής θεώρημα (*πρώτο θεώρημα του Minkowski*):

Θεώρημα 3.1.1 (Minkowski). *Έστω K ανοικτό και φραγμένο, συμμετρικό ως προς το 0, κυρτό υποσύνολο του $\mathbb{R}^n$. Αν $|K| > 2^n$, τότε το K περιέχει τουλάχιστον ένα $u \in \mathbb{Z}^n \setminus \{0\}$.*

Το αποτέλεσμα αυτό δεν επιδέχεται βελτίωση. Αν θεωρήσουμε τον κύβο $Q = \{x : |x_i| < 1, i = 1,\dots,n\}$, τότε $|Q| = 2^n$, αλλά $Q \cap \mathbb{Z}^n = \{0\}$.

Θα δώσουμε μία απόδειξη του Θεωρήματος 3.1.1 η οποία βασίζεται στο εξής Λήμμα του Blichfeldt:

Θεώρημα 3.1.2 (Blichfeldt). *Έστω M ένα Jordan μετρήσιμο υποσύνολο του $\mathbb{R}^n$, με $|M| > 1$. Υπάρχουν $x \neq y$ στο M ώστε $x - y \in \mathbb{Z}^n$.*

Απόδειξη. Η απόδειξη που θα δώσουμε οφείλεται στον Hajos. Υποθέτουμε ότι $|M| > 1$. Αν το M δεν είναι φραγμένο, παρατηρούμε ότι η τομή του M με μπάλα κατάλληλα μεγάλης ακτίνας εξακολουθεί να έχει όγκο μεγαλύτερο από 1. Υποθέτουμε λοιπόν, χωρίς περιορισμό της γενικότητας, ότι το M είναι φραγμένο. Θεωρούμε το θεμελιώδες παραλληλεπίπεδο του $\mathbb{Z}^n$

$$P = \{x \in \mathbb{R}^n : 0 \leq x_i < 1, i = 1,\dots,n\}. \tag{3.1.3}$$

Το σύνολο U των $u \in \mathbb{Z}^n$ για τα οποία $(u+P) \cap M \neq \emptyset$ είναι πεπερασμένο: αν $(u+P) \cap M \neq \emptyset$ τότε $u \in M - P$ και το $M - P$ είναι φραγμένο, άρα έχουμε πεπερασμένες το πλήθος επιλογές για το u. Γράφουμε

$$U = \{u_1, \ldots, u_r\}. \tag{3.1.4}$$

Για κάθε $j = 1, \ldots, r$, ορίζουμε $M_j = (u_j + P) \cap M$. Τα σύνολα M_j είναι ξένα και η ένωσή τους είναι το M. Για κάθε $j = 1, \ldots, r$ θεωρούμε τη μεταφορά $M_j' = M_j - u_j = P \cap (M - u_j) \subseteq P$. Παρατηρούμε ότι $|M_j'| = |M_j|$ για κάθε $j = 1, \ldots, r$. Συνδυάζοντας αυτές τις παρατηρήσεις βλέπουμε ότι αν τα M_j' ήταν ξένα, τότε θα είχαμε

$$\begin{aligned} |P| &\geq |M_1' \cup \cdots \cup M_r'| = \sum_{j=1}^r |M_j'| = \sum_{j=1}^r |M_j| = \sum_{j=1}^r |(u_j + P) \cap M| \\ &= \sum_{u \in \mathbb{Z}^n} |(u+P) \cap M| = |M| > 1, \end{aligned}$$

το οποίο είναι άτοπο. Άρα, υπάρχουν $i \neq j \in \{1, \ldots, r\}$ και $z \in M_i' \cap M_j'$. Τότε, τα $x = z + u_i$ και $y = z + u_j$ ανήκουν στο M, και $x - y = u_i - u_j \in \mathbb{Z}^n \setminus \{0\}$. □

Παρατήρηση. Το ίδιο ισχύει αν υποθέσουμε ότι το M είναι φραγμένο, κλειστό, και $|M| \geq 1$. Γιατί αν πάρουμε μία φθίνουσα ακολουθία $\lambda_r \to 1$, έχουμε $|\lambda_r M| > 1$, άρα υπάρχουν $x_r, y_r \in \lambda_r M$ ώστε $0 \neq x_r - y_r \in \mathbb{Z}^n$. Τότε, οι (x_r), (y_r) έχουν υπακολουθίες $x_{k_r} \to x \in M$, $y_{k_r} \to y \in M$, και εύκολα ελέγχουμε ότι $x - y \in \mathbb{Z}^n \setminus \{0\}$.

Απόδειξη του θεωρήματος 3.1.1. Θεωρούμε το $M = K/2$. Το M είναι Jordan μετρήσιμο και, από την υπόθεσή μας, $|M| > 1$. Από το Λήμμα του Blichfeldt, υπάρχουν $x, y \in M$ ώστε $0 \neq x - y \in \mathbb{Z}^n$. Όμως, από τον ορισμό του M, υπάρχουν $w_1, w_2 \in K$ με $x = w_1/2$ και $y = w_2/2$. Το K είναι συμμετρικό ως προς το 0, άρα $-w_2 \in K$. Από την κυρτότητα του K συμπεραίνουμε ότι

$$x - y = \frac{w_1 + (-w_2)}{2} \in K. \tag{3.1.5}$$

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

3.1.1 Το επιχείρημα του Minkowski

Περιγράφουμε τώρα το αρχικό επιχείρημα του Minkowski. Θεωρούμε ένα κλειστό, συμμετρικό ως προς το 0, κυρτό σώμα K. Για κάθε $\lambda > 0$, θεωρούμε το σώμα λK. Αφού το K είναι φραγμένο, για μικρά λ έχουμε $\lambda K \cap \mathbb{Z}^n = \{0\}$, και αφού το K περιέχει μία μπάλα με κέντρο το 0, για μεγάλα λ θα έχουμε $\lambda K \cap (\mathbb{Z}^n \setminus \{0\}) \neq \emptyset$.

Αφού $0 \in \lambda K$, από την κυρτότητα του K έπεται ότι: αν $0 < \lambda < \lambda'$, τότε $\lambda K \subset \lambda' K$. Αφού το K είναι κλειστό, συμπεραίνουμε ότι

$$\lambda K = \bigcap \{\lambda' K : \lambda' > \lambda\}. \tag{3.1.6}$$

για κάθε $\lambda > 0$. Ειδικότερα, αν ορίσουμε

$$\lambda_1 = \inf\{\lambda > 0 : \lambda K \cap (\mathbb{Z}^n \setminus \{0\}) \neq \emptyset\}, \tag{3.1.7}$$

τότε

$$\lambda_1 K \cap (\mathbb{Z}^n \setminus \{0\}) \neq \emptyset. \tag{3.1.8}$$

Δηλαδή, υπάρχει ελάχιστος $\lambda_1 > 0$ για τον οποίο το $\lambda_1 K$ περιέχει μη μηδενικό ακέραιο σημείο (το οποίο, βέβαια, θα βρίσκεται στο σύνορό του). Για την απόδειξη της (3.1.8), σταθεροποιούμε $\lambda_* > \lambda_1$ και θεωρούμε φθίνουσα ακολουθία $\lambda_* > \mu_n \to \lambda_1$. Το $\lambda_* K$ περιέχει πεπερασμένα το πλήθος μη μηδενικά ακέραια σημεία, και, για κάθε n, κάποιο από αυτά ανήκει στο $\mu_n K$. Υπάρχουν λοιπόν μη μηδενικό $u \in \mathbb{Z}^n$ και υπακολουθία μ_{k_n} ώστε $u \in \mu_{k_n} K$ για κάθε n. Τότε,

$$u \in \bigcap_n \mu_{k_n} K = \lambda_1 K. \tag{3.1.9}$$

Για κάθε $\lambda > 0$ θεωρούμε τα σύνολα $\lambda K + u$, $u \in \mathbb{Z}^n$. Για μικρά λ, τα σύνολα $\lambda K + u$ είναι ξένα ανά δύο. Με ένα επιχείρημα ανάλογο προς το προηγούμενο, δείχνουμε ότι υπάρχει ελάχιστος $\lambda_0 > 0$ για τον οποίο υπάρχει $u \in \mathbb{Z}^n \setminus \{0\}$ ώστε $\lambda_0 K \cap (\lambda_0 K + u) \neq \emptyset$.

Λήμμα 3.1.3. *Για κάθε συμμετρικό κυρτό σώμα K ισχύει η ισότητα $\lambda_1 = 2\lambda_0$.*

Απόδειξη. Έστω $x \in \lambda_0 K \cap (\lambda_0 K + u)$, όπου $u \in \mathbb{Z}^n \setminus \{0\}$. Τότε, λόγω της συμμετρίας του K, έχουμε $u - x \in \lambda_0 K$ και $x \in \lambda_0 K$, άρα $u \in 2\lambda_0 K$. Επομένως,

$$\lambda_1 \leq 2\lambda_0. \tag{3.1.10}$$

Από την άλλη πλευρά, αν $u \in \lambda_1 K \cap (\mathbb{Z}^n \setminus \{0\})$, τότε, παρατηρώντας ότι $-u/2 \in (\lambda_1/2)K$ και χρησιμοποιώντας τη συμμετρία του K, γράφουμε

$$\frac{u}{2} = -\frac{u}{2} + u \in \frac{\lambda_1}{2} K \cap \left(\frac{\lambda_1}{2} K + u \right). \tag{3.1.11}$$

Έπεται ότι $\lambda_0 \leq \lambda_1/2$. □

Ο Minkowski ολοκλήρωνε το επιχείρημά του ως εξής: τα σύνολα $\lambda_0 K + u$, $u \in \mathbb{Z}^n$, έχουν ξένα εσωτερικά. Αυτό έχει σαν συνέπεια την ανισότητα $|\lambda_0 K| \leq 1$ (αλλιώς, το Λήμμα του Blichfeldt θα μας οδηγούσε σε άτοπο, εξηγήστε γιατί). Σύμφωνα με το Λήμμα 3.1.3,

$$\lambda_1^n |K| = |\lambda_1 K| = |(2\lambda_0)K| = 2^n |\lambda_0 K| \leq 2^n. \tag{3.1.12}$$

Αν υποθέσουμε ότι το K δεν περιέχει μη μηδενικό ακέραιο σημείο, τότε $\lambda_1 > 1$, δηλαδή $|K| < 2^n$. Επομένως, κάθε κλειστό, συμμετρικό ως προς το 0 κυρτό σώμα K με όγκο $|K| \geq 2^n$, περιέχει μη μηδενικό $u \in \mathbb{Z}^n$.

Για την περίπτωση του ανοικτού K, υποθέτοντας ότι $|K| > 2^n$, βρίσκουμε $\lambda < 1$ ώστε $\lambda^n |K| > 2^n$, οπότε $|\lambda \overline{K}| = \lambda^n |K| > 2^n$. Εφαρμόζοντας το προηγούμενο αποτέλεσμα, βρίσκουμε μη μηδενικό ακέραιο σημείο $u \in \lambda \overline{K} \subset K$. □

Παρατηρήσεις. Το επιχείρημα του Minkowski (ειδικότερα η εισαγωγή των παραμέτρων λ_0, λ_1 και το Λήμμα 3.1.3) είναι σημαντικό για ιστορικούς λόγους. Τον οδήγησε στον ορισμό της **νόρμας που επάγεται από το K** και στον ορισμό των **διαδοχικών ελαχίστων** του K:

1. Έστω K κλειστό κυρτό υποσύνολο του $\mathbb{R}^n$ με $0 \in \operatorname{int}(K)$. Η *συνάρτηση στάθμης* (ή *συναρτησοειδές Minkowski*) του K είναι η συνάρτηση $g_K : \mathbb{R}^n \to \mathbb{R}$ που ορίζεται από την

$$g_K(x) = \inf\{\lambda > 0 : x \in \lambda K\}. \tag{3.1.13}$$

Αν το K είναι συμμετρικό κυρτό σώμα, τότε η g_K είναι νόρμα στον $\mathbb{R}^n$ και $K = \{x : g_K(x) \leq 1\}$.

2. Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Μπορούμε να ελέγξουμε ότι, για κάθε $i = 1,\dots,n$, υπάρχουν $\lambda > 0$ ώστε το λK να περιέχει τουλάχιστον i γραμμικά ανεξάρτητα διανύσματα του $\mathbb{Z}^n$. Ορίζουμε

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^n) \geq i\}, \tag{3.1.14}$$

όπου $\dim(\lambda K \cap \mathbb{Z}^n)$ είναι η διάσταση του υποχώρου που παράγεται από τα ακέραια σημεία του λK. Οι αριθμοί $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ είναι τα *διαδοχικά ελάχιστα* του K. Σύμφωνα με το πρώτο θεώρημα του Minkowski, αφού $\lambda_1 K \cap \mathbb{Z}^n = \{0\}$, το $\lambda_1 K$ πρέπει να έχει όγκο το πολύ ίσο με 2^n:

$$\lambda_1^n |K| \leq 2^n. \tag{3.1.15}$$

Παίρνοντας υπ' όψιν του όλα τα διαδοχικά ελάχιστα $\lambda_1,\dots,\lambda_n$ του K, ο Minkowski απέδειξε κάτι ισχυρότερο (το *δεύτερο θεώρημα του Minkowski*):

Θεώρημα 3.1.4. *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε,*

$$\lambda_1\lambda_2\dots\lambda_n|K| \leq 2^n. \tag{3.1.16}$$

3.2 Εφαρμογές στη θεωρία των αριθμών

3.2.1 Ομογενείς γραμμικές μορφές

Η πιο γνωστή εφαρμογή του θεωρήματος του Minkowski αφορά συστήματα ομογενών γραμμικών μορφών:

Θεώρημα 3.2.1. *Έστω $\xi_i(x_1,\dots,x_n) = a_{i1}x_1 + \cdots + a_{in}x_n$, $i = 1,\dots,n$, ομογενείς γραμμικές μορφές με πραγματικούς συντελεστές a_{ij} και μη μηδενική ορίζουσα Δ. Αν $t_1,\dots,t_n > 0$ και $t_1t_2\cdots t_n \geq |\Delta|$, τότε υπάρχει $(x_1,\dots,x_n) \in \mathbb{Z}^n \setminus \{0\}$ ώστε*

$$|\xi_i(x_1,\dots,x_n)| \leq t_i, \quad i = 1,\dots,n. \tag{3.2.1}$$

Απόδειξη. Θεωρούμε το παραλληλεπίπεδο

$$P = \{x : |\xi_i(x_1,\dots,x_n)| \leq t_i, i = 1,\dots,n\}. \tag{3.2.2}$$

Αν T είναι ο γραμμικός μετασχηματισμός που ορίζεται από τον πίνακα (a_{ij}), τότε $P = T^{-1}(P_1)$, όπου

$$P_1 = \{y : |y_i| \leq t_i, i = 1,\dots,n\}. \tag{3.2.3}$$

Άρα,

$$|P| = |T^{-1}(P_1)| = \frac{|P_1|}{|\Delta|} = 2^n\frac{t_1t_2\cdots t_n}{|\Delta|} \geq 2^n. \tag{3.2.4}$$

Από το θεώρημα του Minkowski, υπάρχει $x \in P \cap (\mathbb{Z}^n \setminus \{0\})$. □

Εφαρμογή. *Έστω $a_1,\dots,a_n \in \mathbb{R}$. Υπάρχουν ακέραιοι $u_1,\dots,u_{n+1}$ ώστε*

$$|u_{n+1}a_i - u_i| \leq \frac{1}{u_{n+1}^{1/n}}, \quad i = 1,\dots,n. \tag{3.2.5}$$

Απόδειξη. Θέτουμε $\xi_{n+1}(x_1,\dots,x_{n+1}) = x_{n+1}$ και

$$\xi_i(x_1,\dots,x_{n+1}) = x_{n+1}a_i - x_i, \quad i = 1,\dots,n. \tag{3.2.6}$$

Τότε $|\Delta| = 1$, άρα για κάθε $t > 1$ υπάρχει $(u_1,\dots,u_{n+1}) \in \mathbb{Z}^n \setminus \{0\}$ που ικανοποιεί τις

$$|u_{n+1}| \leq t \quad \text{και} \quad |u_{n+1}a_i - u_i| \leq t^{-1/n}. \tag{3.2.7}$$

Το u_{n+1} δεν μπορεί να είναι ίσο με μηδέν, γιατί τότε όλοι οι u_i, $i \leq n$ θα ήταν απολύτως μικρότεροι του 1, δηλαδή επίσης ίσοι με μηδέν. Επίσης, αντικαθιστώντας αν χρειαστεί όλους τους u_i με τους $-u_i$, μπορούμε να υποθέσουμε ότι $u_{n+1} > 0$. Έπεται ότι

$$|u_{n+1}a_i - u_i| \leq \frac{1}{t^{1/n}} \leq \frac{1}{u_{n+1}^{1/n}} \tag{3.2.8}$$

για κάθε $i = 1,\dots,n$. □

3.2.2 Το θεώρημα προσέγγισης του Dirichlet

Εφαρμόζουμε τώρα πιο προσεκτικά το θεώρημα του Minkowski στο πρόβλημα της προσέγγισης πραγματικών αριθμών από ρητούς (θεώρημα του Dirichlet):

Θεώρημα 3.2.2. *Υπάρχει σταθερά $c > 0$ με την ιδιότητα: για κάθε $a \in \mathbb{R}$, υπάρχει οσοδήποτε μεγάλος $q \in \mathbb{N}$ και υπάρχει $p \in \mathbb{Z}$, ώστε*

$$\left|a - \frac{p}{q}\right| \leq \frac{c}{q^2}. \tag{3.2.9}$$

Απόδειξη. Μπορούμε να υποθέσουμε ότι ο a είναι άρρητος (αν ο a είναι ρητός, τότε το πρόβλημα δεν έχει καμιά δυσκολία). Έστω $M > 0$. Αφού $a \notin \mathbb{Q}$, υπάρχει $Q > 1$ ώστε

$$t_M := \min\{|aq - p| : q \leq M, q \in \mathbb{N}, p \in \mathbb{Z}\} > \frac{1}{Q}. \tag{3.2.10}$$

Ορίζουμε

$$K = \left\{(x,y) \in \mathbb{R}^2 : |ax - y| \leq \frac{1}{Q}, |x| \leq Q\right\}. \tag{3.2.11}$$

Το K είναι παραλληλόγραμμο, με εμβαδόν $|K| = (2Q)(2/Q) = 4$. Από το θεώρημα του Minkowski, υπάρχει $(q,p) \in K \cap (\mathbb{Z}^2 \setminus \{0\})$. Έχουμε $q \neq 0$, γιατί αλλιώς θα είχαμε $|p| \leq 1/Q < 1$, δηλαδή $p = 0$. Επίσης, λόγω της συμμετρίας του K, μπορούμε να υποθέσουμε ότι $q > 0$ (δηλαδή, $q \in \mathbb{N}$). Αυτό σημαίνει ότι $0 < q \leq Q$ και $|aq - p| \leq 1/Q$, άρα

$$\left|a - \frac{p}{q}\right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}. \tag{3.2.12}$$

Τέλος, από τον ορισμό του t_M, έχουμε

$$|aq - p| \leq \frac{1}{Q} < t_M, \tag{3.2.13}$$

άρα $q > M$. □

Το Θεώρημα 3.2.2 γενικεύεται ως εξής:

Θεώρημα 3.2.3. *Υπάρχει σταθερά $c > 0$ με την ιδιότητα: αν $a_1, \dots, a_n \in \mathbb{R}$, υπάρχει οσοδήποτε μεγάλος $q \in \mathbb{N}$ και υπάρχουν $p_1, \dots, p_n \in \mathbb{Z}$, ώστε*

$$\left| a_i - \frac{p_i}{q} \right| \leq \frac{c}{q^{1+\frac{1}{n}}}. \tag{3.2.14}$$

Απόδειξη. Έστω $M > 0$. Η απόδειξη είναι εντελώς ανάλογη με αυτήν του Θεωρήματος 3.2.2: μπορούμε να υποθέσουμε ότι οι $a_1, \dots, a_n$ δεν είναι όλοι ρητοί. Το παραλληλεπίπεδο στο οποίο εφαρμόζουμε το Θεώρημα του Minkowski, είναι το

$$K = \left\{ (x, y_1, \dots, y_n) \in \mathbb{R}^{n+1} : |a_i x - y_i| \leq \frac{1}{Q^{1/n}}, |x| \leq Q \right\}, \tag{3.2.15}$$

όπου $Q > 1$ αρκετά μεγάλος ώστε να ικανοποιείται η

$$t_M := \min \left\{ \max_{i \leq n} |a_i q - p_i| : q \leq M, q \in \mathbb{N}, p_i \in \mathbb{Z} \right\} > \frac{1}{Q^{1/n}}. \tag{3.2.16}$$

Οι λεπτομέρειες αφήνονται ως άσκηση. □

3.2.3 Γινόμενο γραμμικών μορφών

Έστω $\xi_i(x_1, \dots, x_n) = a_{i1}x_1 + \cdots + a_{in}x_n$, $i = 1, \dots, n$, ομογενείς γραμμικές μορφές με πραγματικούς συντελεστές a_{ij} και μη μηδενική ορίζουσα Δ. Παίρνοντας $t_1 = \cdots = t_n = |\Delta|^{1/n}$ στο Θεώρημα 3.2.1, βλέπουμε ότι υπάρχει $(x_1, \dots, x_n) \in \mathbb{Z}^n \setminus \{0\}$ ώστε

$$\prod_{i=1}^{n} |\xi_i(x_1, \dots, x_n)| \leq |\Delta|. \tag{3.2.17}$$

Θα δώσουμε ένα καλύτερο άνω φράγμα για το γινόμενο των ξ_i:

Θεώρημα 3.2.4. *Αν ξ_i και Δ όπως παραπάνω, υπάρχει $(x_1, \dots, x_n) \in \mathbb{Z}^n \setminus \{0\}$ ώστε*

$$\prod_{i=1}^{n} |\xi_i(x_1, \dots, x_n)| \leq \frac{n!}{n^n} |\Delta|. \tag{3.2.18}$$

Απόδειξη. Το χωρίο $\{x : \prod_{i=1}^{n} |\xi_i(x)| \leq r\}$, $r > 0$, δεν είναι κυρτό, περιέχει όμως το

$$K_r = \left\{ x \in \mathbb{R}^n : \sum_{i=1}^{n} |\xi_i(x)| \leq n r^{1/n} \right\}, \tag{3.2.19}$$

γιατί, από την ανισότητα αριθμητικού-γεωμετρικού μέσου, για κάθε $x_1, \dots, x_n \in \mathbb{R}$ έχουμε

$$\prod_{i=1}^{n} |\xi_i(x)| \leq \left(\frac{1}{n} \sum_{i=1}^{n} |\xi_i(x)| \right)^n. \tag{3.2.20}$$

Αν T είναι ο γραμμικός μετασχηματισμός που ορίζεται από τις ξ_i, τότε $K_r = T^{-1}(K_r^1)$, όπου

$$K_r^1 = \left\{ y : \sum_{i=1}^{n} |y_i| \leq n r^{1/n} \right\}. \tag{3.2.21}$$

Άρα,

$$|K_r| = \frac{|K_r^1|}{|\det T|} = \frac{2^n n^n r}{n!|\Delta|}. \tag{3.2.22}$$

Ο όγκος του K_r θα είναι ίσος με 2^n αν $r = r_0 = n!|\Delta|/n^n$, και τότε, το θεώρημα του Minkowski μας εξασφαλίζει ότι υπάρχει $x \in K_{r_0} \cap (\mathbb{Z}^n \setminus \{0\})$. Δηλαδή, υπάρχει $x \in \mathbb{Z}^n \setminus \{0\}$ για το οποίο

$$\prod_{i=1}^n |\xi_i(x)| \leq \left(\frac{1}{n}\sum_{i=1}^n |\xi_i(x)|\right)^n \leq r_0 = \frac{n!}{n^n}|\Delta|. \tag{3.2.23}$$

3.2.4 Τετραγωνικές μορφές

Θεώρημα 3.2.5. *Έστω $A = (a_{ij})$ συμμετρικός, θετικά ορισμένος $n\times n$ πίνακας. Θεωρούμε την τετραγωνική μορφή*

$$T(x_1,\dots,x_n) = T(x) = \langle Ax, x\rangle. \tag{3.2.24}$$

Αν $D = \det(a_{ij})$ είναι η διακρίνουσα της T, μπορούμε να βρούμε $(u_1,\dots,u_n) \in \mathbb{Z}^n \setminus \{0\}$ ώστε

$$T(u_1,\dots,u_n) \leq \frac{4}{\pi}\left(\Gamma\left(\frac{n}{2}+1\right)^2 D\right)^{1/n}. \tag{3.2.25}$$

Απόδειξη. Υπάρχει συμμετρικός, θετικά ορισμένος S ώστε $S^2 = A$. Για κάθε $r > 0$ ορίζουμε

$$K_r = \{x \in \mathbb{R}^n : T(x) \leq r\}. \tag{3.2.26}$$

Έχουμε $T(x) \leq r$ αν και μόνο αν $\|Sx\|_2^2 \leq r$. Δηλαδή, $K_r = \sqrt{r}S^{-1}(B_2^n)$. Επομένως,

$$|K_r| = \frac{r^{n/2}}{\det(S)}\omega_n = \frac{r^{n/2}}{\sqrt{D}}\frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}. \tag{3.2.27}$$

Επιλέγουμε $r_0 > 0$ έτσι ώστε να έχουμε $|K_{r_0}| = 2^n$. Τότε, από το Θεώρημα του Minkowski, μπορούμε να βρούμε $(u_1,\dots,u_n) \in K_{r_0} \cap (\mathbb{Z}^n \setminus \{0\})$, δηλαδή,

$$T(u_1,\dots,u_n) \leq r_0 = \frac{4}{\pi}\left(\Gamma\left(\frac{n}{2}+1\right)^2 D\right)^{1/n}. \tag{3.2.28}$$

3.2.5 Το θεώρημα του Lagrange

Χρησιμοποιώντας το θεώρημα του Minkowski, θα αποδείξουμε το εξής θεώρημα του Lagrange:

Θεώρημα 3.2.6. *Κάθε φυσικός αριθμός n γράφεται στη μορφή $n = x_1^2+x_2^2+x_3^2+x_4^2$, όπου $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.*

Απόδειξη. Αρχικά, παρατηρούμε ότι αρκεί να εξετάσουμε την περίπτωση που ο n είναι ελεύθερος τετραγώνων, δηλαδή, $n = p_1 \dots p_r$, όπου p_j διακεκριμένοι πρώτοι. Παρατηρήστε ότι κάθε φυσικός αριθμός n γράφεται στη μορφή $n = s^2 m$, όπου ο m είναι ελεύθερος τετραγώνων ή $m = 1$. Πράγματι, ο n αναλύεται στη μορφή $n = p_1^{a_1}\cdots p_r^{a_r}$. Αν $a_j = 2t_j + v_j$ με $v_j \in \{0,1\}$, αρκεί να θέσουμε $s = p_1^{t_1}\cdots p_r^{t_r}$ και $m = p_1^{v_1}\cdots p_r^{v_r}$.

Αν ο ισχυρισμός του θεωρήματος αληθεύει για τους φυσικούς που είναι ελεύθεροι τετραγώνων, και αν μας δοθεί τυχών φυσικός αριθμός n, γράφουμε τον n στη μορφή $n = s^2 m$ όπου ο m είναι ελεύθερος τετραγώνων και, γνωρίζοντας ότι μπορούμε να γράψουμε τον m στη μορφή $m = y_1^2 + y_2^2 + y_3^2 + y_4^2$ όπου $y_i \in \mathbb{Z}$, παίρνουμε

$$n = (ly_1)^2 + (ly_2)^2 + (ly_3)^2 + (ly_4)^2.$$

Υποθέτουμε λοιπόν ότι $n = p_1 \dots p_r$, όπου p_j διακεκριμένοι πρώτοι.

Λήμμα 3.2.7. *Έστω p πρώτος. Υπάρχουν $a_p, b_p \in \mathbb{Z}$ ώστε*

$$a_p^2 + b_p^2 + 1 \equiv 0 \pmod{p}. \tag{3.2.29}$$

Απόδειξη. Αν $p = 2$, παίρνουμε $a_2 = 1$ και $b_2 = 0$. Αν ο p είναι περιττός πρώτος, ελέγχουμε ότι οι αριθμοί a^2, $a = 0, 1, \dots, \frac{p-1}{2}$, είναι ανισοϋπόλοιποι $\bmod p$, και το ίδιο ισχύει για τους $-1 - b^2$, $b = 0, 1, \dots, \frac{p-1}{2}$. Αφού το πλήθος των a και b είναι $p + 1$, υπάρχουν δύο από αυτούς που ανήκουν στην ίδια κλάση $\bmod p$. Αυτό σημαίνει υποχρεωτικά ότι υπάρχουν $0 \le a_p, b_p \le \frac{p-1}{2}$ με την ιδιότητα

$$a_p^2 \equiv -1 - b_p^2 \pmod{p}, \tag{3.2.30}$$

δηλαδή, $a_p^2 + b_p^2 + 1 \equiv 0 \pmod{p}$. □

Λήμμα 3.2.8. *Έστω $n = p_1 \dots p_r$, όπου p_j διακεκριμένοι πρώτοι. Υπάρχουν $a, b \in \mathbb{Z}$ ώστε*

$$a^2 + b^2 + 1 \equiv 0 \pmod{n}. \tag{3.2.31}$$

Απόδειξη. Από το προηγούμενο λήμμα, για κάθε $j = 1, \dots, r$ υπάρχουν $a_j, b_j \in \mathbb{Z}$ ώστε

$$a_j^2 + b_j^2 + 1 \equiv \pmod{p_j}. \tag{3.2.31}$$

Από το Κινέζικο Θεώρημα Υπολοίπων, τα συστήματα

$$x \equiv a_j \pmod{p_j}, \qquad j = 1, \dots, r$$

και

$$x \equiv b_j \pmod{p_j}, \qquad j = 1, \dots, r$$

έχουν λύσεις a και b αντίστοιχα. Τότε,

$$a^2 + b^2 + 1 \equiv a_j^2 + b_j^2 + 1 \equiv \pmod{p_j} \tag{3.2.32}$$

για κάθε $j = 1, \dots, r$. Αφού οι p_j είναι διακεκριμένοι πρώτοι, έπεται ότι $a^2 + b^2 + 1 \equiv 0 \pmod{n}$. □

Συνέχεια της απόδειξης του θεωρήματος. Θα λέμε **πλέγμα** κάθε σύνολο της μορφής $\Lambda = T(\mathbb{Z}^n)$, όπου $T \in GL(n)$ (ο T είναι αντιστρέψιμος γραμμικός μετασχηματισμός του $\mathbb{R}^n$). Αν για κάποιο πλέγμα $\Lambda = T(\mathbb{Z}^n)$ και κάποιο συμμετρικό κυρτό σώμα K στον $\mathbb{R}^n$ ισχύει

$$|K| \ge 2^n |\det T|, \tag{3.2.33}$$

τότε υπάρχει $v \neq 0$ ώστε $v \in K \cap \Lambda$. Πράγματι, αν θεωρήσουμε το συμμετρικό κυρτό σώμα $K_1 = T^{-1}(K)$, τότε $|K_1| = |K|/|\det T| \ge 2^n$. Από το θεώρημα του Minkowski υπάρχει $u \neq 0$ ώστε $u \in K_1 \cap \mathbb{Z}^n$. Θέτοντας $v = T(u)$ έχουμε $v \neq 0$, $v \in T(K_1) = K$ και $v \in T(\mathbb{Z}^n) = \Lambda$.

Από το Λήμμα 3.2.8 υπάρχουν $a,b \in \mathbb{Z}$ ώστε $n \mid (a^2+b^2+1)$. Θεωρούμε τον γραμμικό μετασχηματισμό $T:\mathbb{R}^4 \to \mathbb{R}^4$ που ορίζεται από τις

$$T(e_1)=(1,0,a,-b),\ T(e_2)=(0,1,b,a),\ T(e_3)=(0,0,n,0),\ T(e_4)=(0,0,0,n).$$

Ο T είναι αντιστρέψιμος και $|\det T| = n^2$. Αν $u=(u_1,u_2,u_3,u_4)\in\mathbb{Z}^n$ τότε

$$T(u)=(u_1,u_2,au_1+bu_2+nu_3,-bu_1+au_2+nu_4). \tag{3.2.34}$$

Θεωρούμε το πλέγμα $\Lambda = T(\mathbb{Z}^n)$ και τη μπάλα $B=\{x : x_1^2+x_2^2+x_3^2+x_4^2<2n\}$. Ο όγκος της είναι ίσος με

$$|B| = 2n^2\pi^2 > 16n^2 = 2^4|\det T|. \tag{3.2.35}$$

Από το θεώρημα του Minkowski, υπάρχει $(x_1,x_2,x_3,x_4)\in\Lambda\setminus\{0\}$ ώστε

$$0<x_1^2+x_2^2+x_3^2+x_4^2<2n. \tag{3.2.36}$$

Δηλαδή, υπάρχει $u\in\mathbb{Z}^n\setminus\{0\}$ ώστε

$$0<u_1^2+u_2^2+(au_1+bu_2+nu_3)^2+(-bu_1+au_2+nu_4)^2<2n. \tag{3.2.37}$$

Όμως, αν θέσουμε $U=u_1^2+u_2^2+(au_1+bu_2+nu_3)^2+(-bu_1+au_2+nu_4)^2$, έχουμε

$$\begin{aligned} U &\equiv u_1^2+u_2^2+(au_1+bu_2)^2+(-bu_1+au_2)^2 \pmod n \\ &\equiv u_1^2+u_2^2+(a^2+b^2)(u_1^2+u_2^2) \pmod n \\ &\equiv (a^2+b^2+1)(u_1^2+u_2^2) \pmod n \\ &\equiv 0 \pmod n \end{aligned}$$

Άρα, $n\mid U$. Από την (3.2.37) συμπεραίνουμε ότι $n=U=u_1^2+u_2^2+(au_1+bu_2+nu_3)^2+(-bu_1+au_2+nu_4)^2$. □

3.3 Ακέραια σημεία σε ελλειψοειδή

Ένα συμμετρικό κυρτό σώμα E στον $\mathbb{R}^n$ λέγεται **ελλειψοειδές** αν υπάρχει αντιστρέψιμος γραμμικός μετασχηματισμός T ($T\in GL(n)$) ώστε $E=T(B_2^n)$.

Συμβολίζουμε με $\mathcal{E}_n$ την κλάση όλων των ελλειψοειδών του $\mathbb{R}^n$ που δεν περιέχουν στο εσωτερικό τους κανένα σημείο του $\mathbb{Z}^n\setminus\{0\}$. Το πρόβλημα που θα μάς απασχολήσει σε αυτή την Παράγραφο είναι να δοθούν εκτιμήσεις για την ποσότητα

$$\alpha_n = \sup\{|E| : E\in\mathcal{E}_n\}. \tag{3.3.1}$$

3.3.1 Η μέθοδος του Blichfeldt

Ο Blichfeldt έδωσε το ακόλουθο άνω φράγμα για την α_n.

Θεώρημα 3.3.1. *Για κάθε $n\in\mathbb{N}$, ισχύει η ανισότητα*

$$\alpha_n \le \frac{n+2}{2}2^{n/2}. \tag{3.3.2}$$

Για την απόδειξη της ανισότητας κάνουμε πρώτα την εξής αναγωγή. Θέλουμε να δείξουμε ότι:

Για κάθε ελλειψοειδές E με όγκο $|E| > \frac{n+2}{2}2^{n/2}$ ισχύει $E \cap (\mathbb{Z}^n \setminus \{0\}) \neq \emptyset$.

Ισοδύναμα, αρκεί να δείξουμε ότι:

Για κάθε πλέγμα $\Lambda = T(\mathbb{Z}^n)$ στον $\mathbb{R}^n$ με $|B_2^n| > \frac{n+2}{2}|\det T|$ ισχύει $B_2^n \cap (\Lambda \setminus \{0\}) \neq \emptyset$.

Η απόδειξη της ισοδυναμίας των δύο προτάσεων αφήνεται ως άσκηση.

Θεωρούμε λοιπόν ένα πλέγμα $\Lambda = T(\mathbb{Z}^n)$ στον $\mathbb{R}^n$ το οποίο ικανοποιεί την

$$|B_2^n| > \frac{n+2}{2}|\det T|. \tag{3.3.3}$$

Αν $v_i = T(e_i)$, $i = 1, \dots, n$, θεωρούμε το παραλληλεπίπεδο

$$Q = \left\{ \sum_{i=1}^{n} t_i v_i : \ 0 \leq t_i < 1 \right\}. \tag{3.3.4}$$

Παρατηρήστε ότι $Q = T(P)$, όπου $P = \{x : 0 \leq x_i < 1, i = 1, \dots n\}$ είναι το θεμελιώδες παραλληλεπίπεδο του $\mathbb{Z}^n$. Συνεπώς,

$$|Q| = |T(P)| = |\det T|\,|P| = |\det T|. \tag{3.3.5}$$

Για κάθε ολοκληρώσιμη συνάρτηση $f : \mathbb{R}^n \to \mathbb{R}$ μπορούμε να γράψουμε

$$\begin{aligned} \int\limits_{\mathbb{R}^n} f(x)\,dx &= \sum_{u\in\Lambda} \int\limits_{u+Q} f(x)\,dx = \sum_{u\in\Lambda} \int\limits_{Q} f(u+y)\,dy \\ &= \int\limits_{Q} \left(\sum_{u\in\Lambda} f(u+y) \right) dy. \end{aligned}$$

Αν λοιπόν η f ικανοποιεί την

$$\int\limits_{\mathbb{R}^n} f(x)\,dx > |Q|, \tag{3.3.6}$$

τότε

$$\frac{1}{|Q|} \int\limits_{Q} \left(\sum_{u\in\Lambda} f(u+y) \right) dy > 1, \tag{3.3.7}$$

και αυτό σημαίνει ότι υπάρχει $y \in \mathbb{R}^n$ ώστε

$$\sum_{u\in\Lambda} f(u+y) > 1. \tag{3.3.8}$$

Λήμμα 3.3.2. *Η συνάρτηση*

$$f(x) = \begin{cases} 1 - 2\|x\|_2^2 & , \ 0 \leq \|x\|_2 < \frac{1}{\sqrt{2}} \\ 0 & , \ \|x\|_2 \geq \frac{1}{\sqrt{2}} \end{cases}$$

ικανοποιεί την

$$\int\limits_{\mathbb{R}^n} f(x)\,dx > |Q|.$$

Απόδειξη. Θέτοντας $r = \frac{1}{\sqrt{2}}$ έχουμε

$$\begin{aligned}
\int\limits_{\mathbb{R}^n} f(x)\,dx &= \int\limits_{rB_2^n} \left(1 - \frac{\|x\|_2^2}{r^2}\right) dx \\
&= |rB_2^n| - \frac{1}{r^2} \int\limits_{rB_2^n} \int\limits_0^{\|x\|_2} 2t\,dt\,dx \\
&= |rB_2^n| - \frac{1}{r^2} \int\limits_0^r 2t \int\limits_{t\le\|x\|_2\le r} dx\,dt \\
&= |rB_2^n| - \frac{1}{r^2} \int\limits_0^r 2t \left(|rB_2^n| - |tB_2^n|\right) dt \\
&= |rB_2^n| - |rB_2^n| \frac{1}{r^2} \int\limits_0^r 2t \left(1 - \frac{t^n}{r^n}\right) dt \\
&= |rB_2^n| - |rB_2^n| \frac{1}{r^2} \int\limits_0^r \left(2t - \frac{2t^{n+1}}{r^n}\right) dt \\
&= |rB_2^n| - |rB_2^n| \left(1 - \frac{2}{n+2}\right) = \frac{2}{n+2}|rB_2^n| \\
&= \frac{2}{n+2}\frac{1}{2^{n/2}}|B_2^n| \\
&> |\det T| = |Q|,
\end{aligned}$$

όπου στο τέλος αντικαταστήσαμε $r = 1/\sqrt{2}$ και χρησιμοποιήσαμε την υπόθεση ότι $|B_2^n| > \frac{n+2}{2}|\det T|$ που κάναμε για το Λ στην (3.3.3). □

Τώρα, μπορούμε να εφαρμόσουμε την (3.3.8) για τη συγκεκριμένη συνάρτηση f: υπάρχει $y \in \mathbb{R}^n$ ώστε

$$\sum_{u\in\Lambda\cap B(-y,1/\sqrt{2})} (1 - 2\|u+y\|_2^2 > 1. \tag{3.3.9}$$

Το σύνολο U των $u \in \Lambda$ που ικανοποιούν την $\|u+y\|_2 < 1/\sqrt{2}$ είναι πεπερασμένο. Μπορούμε λοιπόν να γράψουμε $U = \{u_1, \ldots, u_m\}$ και τότε η (3.3.9) παίρνει τη μορφή

$$\sum_{i=1}^m (1 - 2\|u_i + y\|_2^2) > 1,$$

δηλαδή

$$\sum_{i=1}^m \|u_i + y\|_2^2 < \frac{m-1}{2}. \tag{3.3.10}$$

Ο Blichfeldt ολοκλήρωνε την απόδειξη του θεωρήματος μέσω της ακόλουθης ανισότητας:

Λήμμα 3.3.3. *Αν $y, u_1, \ldots, u_m \in \mathbb{R}^n$, τότε*

$$\sum_{i=1}^m \sum_{j=1}^m \|u_i - u_j\|_2^2 \le 2m \sum_{i=1}^m \|u_i + y\|_2^2. \tag{3.3.11}$$

Απόδειξη. Παρατηρούμε πρώτα ότι αρκεί να αποδείξουμε την ανισότητα στην περίπτωση $y = 0$:

$$\sum_{i=1}^{m}\sum_{j=1}^{m}\|u_i - u_j\|_2^2 \leq 2m\sum_{i=1}^{m}\|u_i\|_2^2. \tag{3.3.12}$$

Κατόπιν εφαρμόζουμε αυτή την ειδική περίπτωση για τα $u_1 + y, \ldots, u_m + y$.

Για την απόδειξη της (3.3.12), γράφουμε

$$\begin{aligned}\sum_{i=1}^{m}\sum_{j=1}^{m}\|u_i - u_j\|_2^2 &= \sum_{i=1}^{m}\sum_{j=1}^{m}\left(\|u_i\|_2^2 - 2\langle u_i, u_j\rangle + \|u_j\|_2^2\right)\\ &= 2m\sum_{i=1}^{m}\|u_i\|_2^2 - 2\Big\langle\sum_{i=1}^{m}u_i, \sum_{j=1}^{m}u_j\Big\rangle\\ &= 2m\sum_{i=1}^{m}\|u_i\|_2^2 - 2\Big\|\sum_{i=1}^{m}u_i\Big\|_2^2\\ &\leq 2m\sum_{i=1}^{m}\|u_i\|_2^2. \qquad \square\end{aligned}$$

Επιστρέφουμε στην (3.3.10): χρησιμοποιώντας το Λήμμα 3.3.3 παίρνουμε

$$\sum_{i,j=1}^{m}\|u_i - u_j\|_2^2 \leq 2m\sum_{i=1}^{m}\|u_i + y\|_2^2 < 2m\frac{m-1}{2} = m(m-1). \tag{3.3.13}$$

Όμως, το πλήθος των μη μηδενικών όρων $\|u_i - u_j\|_2^2$ (με $i \neq j$) στο αριστερό μέλος της (3.3.13) είναι ίσο με $m(m-1)$. Συνεπώς, υπάρχουν $i \neq j$ ώστε $\|u_i - u_j\|_2^2 < 1$. Δηλαδή, το $v = u_i - u_j$ ανήκει στο Λ, είναι μη μηδενικό, και

$$\|v\|_2 = \|u_i - u_j\|_2 < 1.$$

Αυτό σημαίνει ότι $v \in B_2^n \cap (\Lambda \setminus \{0\})$. Δηλαδή, δείξαμε ότι για κάθε πλέγμα $\Lambda = T(\mathbb{Z}^n)$ στον $\mathbb{R}^n$ με $|B_2^n| > \frac{n+2}{2}|\det T|$ ισχύει $B_2^n \cap (\Lambda \setminus \{0\}) \neq \emptyset$. $\square$

3.3.2 Ελλειψοειδή χωρίς ακέραια σημεία

Σε αυτή την παράγραφο εξετάζουμε το αντίστροφο πρόβλημα: να βρεθεί ελλειψοειδές με όσο γίνεται μεγαλύτερο όγκο, το οποίο δεν περιέχει ακέραια σημεία στο εσωτερικό του. Το καλύτερο γνωστό αποτέλεσμα οφείλεται στον K. Ball και χρησιμοποιεί το Λήμμα του Bang:

Λήμμα 3.3.4. *Έστω $x_1, \ldots, x_m$ μοναδιαία διανύσματα στον $\mathbb{R}^n$, και $w_1, \ldots, w_m$ θετικοί πραγματικοί αριθμοί. Υπάρχει επιλογή προσήμων $\varepsilon_1, \ldots, \varepsilon_m \in \{-1, 1\}$ ώστε το $u = \sum_{i=1}^{m}\varepsilon_i w_i x_i$ να ικανοποιεί τις*

$$|\langle u, x_i\rangle| \geq w_i, \quad i = 1, \ldots, m. \tag{3.3.14}$$

Απόδειξη. Για κάθε $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_m) \in \{-1, 1\}^m$, θέτουμε $u(\varepsilon) = \sum_{i=1}^{m}\varepsilon_i w_i x_i$. Επιλέγουμε εκείνο το $u = u(\varepsilon^*)$ που έχει το μεγαλύτερο μήκος (αν υπάρχουν περισσότερα από ένα τέτοια $u(\varepsilon)$, επιλέγουμε οποιοδήποτε από αυτά).

Για κάθε $j = 1, \dots, m$, ορίζουμε

$$u_j = u(\varepsilon^*) - 2\varepsilon_j^* w_j x_j. \tag{3.3.15}$$

Κάθε u_j είναι της μορφής $u(\varepsilon)$, με $\varepsilon_i = \varepsilon_i^*$ αν $i \neq j$, και $\varepsilon_j = -\varepsilon_j^*$. Άρα,

$$\begin{aligned} \|u(\varepsilon^*)\|_2^2 &\geq \|u_j\|_2^2 = \|u(\varepsilon^*) - 2\varepsilon_j^* w_j x_j\|_2^2 \\ &= \|u(\varepsilon^*)\|_2^2 - 4w_j\varepsilon_j^*\langle u(\varepsilon^*), x_j\rangle + 4w_j^2\|x_j\|_2^2. \end{aligned}$$

Έπεται ότι

$$|\langle u(\varepsilon^*), x_j\rangle| \geq \varepsilon_j^*\langle u(\varepsilon^*), x_j\rangle \geq \frac{4w_j^2\|x_j\|_2^2}{4w_j} = w_j, \tag{3.3.16}$$

για κάθε $j = 1, \dots, m$. □

Η ακριβής διατύπωση του θεωρήματος του Ball είναι η εξής:

Θεώρημα 3.3.5. *Για κάθε $\varepsilon > 0$ υπάρχει ελλειψοειδές E στον $\mathbb{R}^n$ που δεν περιέχει σημεία του $\mathbb{Z}^n\setminus\{0\}$, και έχει όγκο*

$$|E| > 2(n-1) - \varepsilon. \tag{3.3.17}$$

Απόδειξη. Θεωρούμε την κλάση όλων των ελλειψοειδών της μορφής

$$E_R = \{x \in \mathbb{R}^n : \langle u, x\rangle^2 + \|x\|_2^2 < R^2\}, \;\; u \in \mathbb{R}^n, R > 0. \tag{3.3.18}$$

Για κάθε $R > 0$, προσπαθούμε αρχικά να βρούμε $u = u_R \in \mathbb{R}^n$, ώστε το E_R να μην περιέχει ακέραια σημεία εκτός από το 0. Δηλαδή, ζητάμε για κάθε $z \in \mathbb{Z}^n \setminus \{0\}$ να ισχύει

$$\langle u, z\rangle^2 + \|z\|_2^2 \geq R^2. \tag{3.3.19}$$

Η ανισότητα αυτή ικανοποιείται προφανώς αν $\|z\|_2 \geq R$. Περιοριζόμαστε λοιπόν στα $0 < \|z\|_2 < R$, και ζητάμε

$$\left|\left\langle u, \frac{z}{\|z\|_2}\right\rangle\right| \geq \sqrt{\frac{R^2}{\|z\|_2^2} - 1}. \tag{3.3.20}$$

Θέτουμε $w_z = \sqrt{(R/\|z\|_2)^2 - 1}$, κρατάμε ένα μόνο $\tilde{z}$ από τα $\pm z$ για κάθε $0 < \|z\|_2 < R$, και εφαρμόζουμε το Λήμμα του Bang: υπάρχουν $\varepsilon_{\tilde{z}} \in \{-1, 1\}$, ώστε

$$\left|\left\langle \sum_{\tilde{z}} \varepsilon_{\tilde{z}} w_{\tilde{z}} \frac{\tilde{z}}{\|\tilde{z}\|_2}, \frac{\tilde{z}}{\|\tilde{z}\|_2}\right\rangle\right| \geq w_{\tilde{z}}, \quad 0 < \|z\|_2 < R. \tag{3.3.21}$$

Ισοδύναμα, υπάρχουν $\varepsilon_z \in \{-1, 1\}$ ώστε το διάνυσμα

$$u = u(R) = \frac{1}{2}\sum_{0<\|z\|_2<R} \varepsilon_z w_z \frac{z}{\|z\|_2} \tag{3.3.22}$$

να ικανοποιεί τις

$$\left|\left\langle u, \frac{z}{\|z\|_2}\right\rangle\right| \geq w_z, \quad 0 < \|z\|_2 < R. \tag{3.3.23}$$

Γι' αυτήν την επιλογή του u έχουμε εξασφαλίσει ότι $E_R \cap \mathbb{Z}^n = \{0\}$. Για τον υπολογισμό του όγκου του E_R, χρειαζόμαστε μία εκτίμηση για το μήκος του u. Για το σκοπό αυτό, θεωρούμε το μοναδιαίο διάνυσμα θ στη διεύθυνση του u. Αν $K(R)$ είναι το μήκος του u, έχουμε

$$\begin{aligned} K(R) = \|u\|_2 = \langle u, \theta \rangle &= \frac{1}{2} \sum_{0<\|z\|_2<R} \varepsilon_z \frac{\langle z, \theta \rangle}{\|z\|_2} w_z \\ &\leq \frac{1}{2} \sum_{0<\|z\|_2<R} \frac{|\langle z, \theta \rangle|}{\|z\|_2} \sqrt{\frac{R^2}{\|z\|_2^2} - 1} =: \tilde{K}(R). \end{aligned}$$

Θέτουμε $v = z/R$. Τότε,

$$\tilde{K}(R) = \frac{1}{2} \sum_{v \in \frac{1}{R}\mathbb{Z}^n \cap B_2^n \setminus \{0\}} \frac{|\langle v, \theta \rangle|}{\|v\|_2} \sqrt{\frac{1}{\|v\|_2^2} - 1}. \tag{3.3.24}$$

Καθώς το $R \to \infty$, το παραπάνω άθροισμα (πολλαπλασιασμένο επί R^{-n}) είναι ένα άθροισμα Riemann για το

$$\frac{1}{2} \int_{B_2^n} \frac{|\langle v, \theta \rangle|}{\|v\|_2} \sqrt{\frac{1}{\|v\|_2^2} - 1}\, dv. \tag{3.3.25}$$

Δηλαδή,

$$\lim_{R\to\infty} \frac{\tilde{K}(R)}{\omega_n R^n} = \frac{1}{2\omega_n} \int_{B_2^n} \frac{|\langle v, \theta \rangle|}{\|v\|_2} \sqrt{\frac{1}{\|v\|_2^2} - 1}\, dv. \tag{3.3.26}$$

Για τον υπολογισμό του τελευταίου ολοκληρώματος, παίρνουμε πολικές συντεταγμένες:

$$\begin{aligned} \lim_{R\to\infty} \frac{\tilde{K}(R)}{\omega_n R^n} &= \frac{n\omega_n}{2\omega_n} \int_{S^{n-1}} \int_0^1 |\langle \phi, \theta \rangle| \rho^{n-1} \sqrt{\frac{1}{\rho^2} - 1} d\rho \sigma(d\phi) \\ &= \frac{n}{2} \int_{S^{n-1}} |\langle \phi, \theta \rangle| \sigma(d\phi) \cdot \int_0^1 \rho^{n-2} \sqrt{1-\rho^2} d\rho. \end{aligned}$$

Παρατηρούμε ότι το πρώτο ολοκλήρωμα είναι ανεξάρτητο του $\theta \in S^{n-1}$. Μπορούμε λοιπόν να υποθέσουμε ότι $\theta = e_1$. Γράφουμε

$$\int_{B_2^n} |z_1| dz = n\omega_n \int_{S^{n-1}} |\langle \phi, e_1 \rangle| \sigma(d\phi) \cdot \int_0^1 \rho^n d\rho = \frac{n\omega_n}{n+1} \int_{S^{n-1}} |\langle \phi, e_1 \rangle| \sigma(d\phi), \tag{3.3.27}$$

και

$$\int_{B_2^n} |z_1| dz = 2 \int_0^1 \omega_{n-1} t (1-t^2)^{(n-1)/2} dt, \tag{3.3.28}$$

οπότε,

$$\int_{S^{n-1}} |\langle \phi, \theta \rangle| \sigma(d\phi) = \frac{2\omega_{n-1} \int_0^1 t(1-t^2)^{(n-1)/2} dt}{(n\omega_n)/(n+1)}$$

$$\begin{aligned} &= \frac{2(n+1)\omega_{n-1}}{n\omega_n}\left[-\frac{1}{n+1}(1-t^2)^{(n+1)/2}\right]_0^1 \\ &= \frac{2\omega_{n-1}}{n\omega_n}. \end{aligned}$$

Τέλος,

$$\int_0^1 \rho^{n-2}\sqrt{1-\rho^2}d\rho = \frac{1}{2}\int_0^1 t^{\frac{n-1}{2}-1}(1-t)^{\frac{3}{2}-1}dt = \frac{\Gamma((n-1)/2)\Gamma(3/2)}{2\Gamma((n+2)/2)}.$$

Παίρνοντας υπ' όψιν μας την $\omega_k = \pi^{k/2}/\Gamma((k/2)+1)$, καταλήγουμε στην

$$\begin{aligned} \lim_{R\to\infty}\frac{\tilde{K}(R)}{\omega_n R^n} &= \frac{2\omega_{n-1}}{n\omega_n}\frac{\Gamma(\frac{n-1}{2})\frac{\sqrt{\pi}}{2}}{\Gamma(\frac{n}{2})} \\ &= \frac{2}{n}\frac{\pi^{(n-1)/2}\Gamma(\frac{n}{2}+1)}{\pi^{n/2}\Gamma(\frac{n-1}{2}+1)}\frac{\Gamma(\frac{n-1}{2})\frac{\sqrt{\pi}}{2}}{2\Gamma(\frac{n}{2})} \\ &= \frac{1}{2(n-1)}. \end{aligned}$$

Αυτό σημαίνει ότι, για μεγάλα R,

$$\frac{\omega_n R^n}{\tilde{K}(R)} > 2(n-1) - \frac{\varepsilon}{2}. \tag{3.3.29}$$

Παρατηρούμε επίσης ότι $\lim \tilde{K}(R) = +\infty$, αλλιώς θα είχαμε

$$\lim_{R\to\infty}\frac{\tilde{K}(R)}{\omega_n R^n} = 0. \tag{3.3.30}$$

Από την άλλη πλευρά, ο όγκος του E_R είναι ίσος με τον όγκο του

$$E_R' = \{x\in\mathbb{R}^n : \langle K(R)e_1, x\rangle^2 + \|x\|_2^2 < R^2\}, \tag{3.3.31}$$

ο οποίος υπολογίζεται εύκολα: το E_R' έχει $(n-1)$ ημιάξονες ίσους με R, και έναν ίσο με $R/\sqrt{1+K^2(R)}$. Άρα,

$$|E_R| = \frac{\omega_n R^n}{\sqrt{1+K^2(R)}} \geq \frac{\omega_n R^n}{\sqrt{1+\tilde{K}^2(R)}}, \tag{3.3.32}$$

το οποίο για μεγάλα R είναι μεγαλύτερο από

$$\frac{\omega_n R^n}{\tilde{K}(R)} - \frac{\varepsilon}{2} > 2(n-1) - \varepsilon. \tag{3.3.33}$$

Έτσι, έχουμε αποδείξει ότι υπάρχουν ελλειψοειδή χωρίς μη τετριμμένα ακέραια σημεία, τα οποία έχουν όγκο οσοδήποτε κοντά στο $2(n-1)$. □

Άμεση συνέπεια είναι το ακόλουθο κάτω φράγμα για την α_n:

Θεώρημα 3.3.6. *Για κάθε $n\in\mathbb{N}$, $\alpha_n \geq 2(n-1)$.* □

Σημείωση. Στην κατεύθυνση του Θεωρήματος του Blichfeldt, το καλύτερο γνωστό αποτέλεσμα είναι αυτό των Kabatjanskii και Levenstein (KL):

$$\alpha_n \leq (1.32)^n \simeq 2^{[0.401+o_n(1)]n}. \tag{3.3.34}$$

3.4 Παράρτημα: εφαρμογές της ανάλυσης Fourier στην κυρτή γεωμετρία

3.4.1 Η απόδειξη του Siegel για το πρώτο θεώρημα του Minkowski

Ο Siegel απέδειξε έναν γενικό τύπο από τον οποίο προκύπτει ως πόρισμα το πρώτο θεώρημα του Minkowski. Η απόδειξη αυτού του τύπου χρησιμοποιεί την ταυτότητα του Parseval. Η ιδέα είναι η εξής:

Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$, χ η χαρακτηριστική συνάρτηση του $K/2$, και

$$\phi(x) = \sum_{u\in\mathbb{Z}^n} \chi(u+x). \tag{3.4.1}$$

Τότε, η $\phi(x_1,\dots,x_n)$ είναι περιοδική ως προς κάθε μεταβλητή, με περίοδο 1. Αν $P = \{x : 0 \le x_i < 1, i = 1,\dots,n\}$ είναι το σύνηθες θεμελιώδες παραλληλεπίπεδο του $\mathbb{Z}^n$, η ταυτότητα του Parseval μας δίνει

$$\int_P \phi^2(x)dx = \sum_{u\in\mathbb{Z}^n} |\alpha(u)|^2, \tag{3.4.2}$$

όπου

$$\begin{aligned}\alpha(u) &= \int_P \phi(x)e^{-2\pi i\langle u,x\rangle}dx = \sum_{u\in\mathbb{Z}^n}\int_P \chi(u+x)e^{-2\pi i\langle u,x\rangle}dx \\ &= \int_{\mathbb{R}^n} \chi(x)e^{-2\pi i\langle u,x\rangle}dx,\end{aligned}$$

είναι οι συντελεστές Fourier της ϕ.

Θεώρημα 3.4.1. *Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$ που δεν περιέχει μη μηδενικό ακέραιο σημείο. Αν ορίσουμε ϕ και α όπως παραπάνω, τότε*

$$2^n = |K| + \frac{4^n}{|K|}\sum_{u\in\mathbb{Z}^n\setminus\{0\}} |\alpha(u)|^2. \tag{3.4.3}$$

Απόδειξη. Αφού $K\cap\mathbb{Z}^n = \{0\}$, τα σύνολα $u + \frac{1}{2}K$, $u\in\mathbb{Z}^n$, είναι ξένα, επομένως

$$u \ne u' \Longrightarrow \chi(x+u)\chi(x+u') = 0. \tag{3.4.4}$$

Έπεται ότι $\phi^2 = \phi$ στον $\mathbb{R}^n$, άρα

$$\alpha(0) = \int_P \phi(x)dx = \int_P \phi^2(x)dx = |\alpha(0)|^2 + \sum_{u\in\mathbb{Z}^n\setminus\{0\}} |\alpha(u)|^2. \tag{3.4.5}$$

Όμως,

$$\alpha(0) = \int_{\mathbb{R}^n} \chi(x)dx = \frac{|K|}{2^n}, \tag{3.4.6}$$

άρα

$$\frac{|K|}{2^n} = \frac{|K|^2}{4^n} + \sum_{u\in\mathbb{Z}^n\setminus\{0\}} |\alpha(u)|^2, \tag{3.4.7}$$

και το ζητούμενο προκύπτει αν πολλαπλασιάσουμε τα δύο μέλη της τελευταίας ισότητας με $4^n/|K|$. □

Πόρισμα 3.4.2. *Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Αν $K\cap\mathbb{Z}^n = \{0\}$, τότε $|K| \le 2^n$.* □

3.4.2 Η απόδειξη του Hurwitz για την ισοπεριμετρική ανισότητα στο επίπεδο

Χρησιμοποιώντας μεθόδους ανάλυσης Fourier, ο Hurwitz απέδειξε την ακόλουθη ισοπεριμετρική ανισότητα:

Θεώρημα 3.4.3. *Εστω K χωρίο στο επίπεδο του οποίου το σύνορο είναι μιά απλή κλειστή και λεία καμπύλη. Τότε,*

$$4\pi A(K) \leq P^2(K),$$

όπου $A(K)$ είναι το εμβαδόν του K και $P(K)$ είναι η περίμετρος του K. Ισότητα ισχύει μόνο αν το K είναι δίσκος.

Αρχικές παρατηρήσεις. Υποθέτουμε ότι το χωρίο K έχει σαν σύνορό του μία λεία απλή κλειστή καμπύλη $\gamma : [a,b] \to \mathbb{R}^2$. Με αυτό εννοούμε ότι αν $\gamma(t) = (x(t), y(t))$, τότε οι x' και y' είναι συνεχείς και επιπλέον $(x'(t), y'(t)) \neq (0,0)$ γιά κάθε t, το οποίο εξασφαλίζει ότι η καμπύλη έχει σε κάθε σημείο εφαπτόμενο διάνυσμα το οποίο μεταβάλλεται με συνεχή τρόπο.

Το μήκος της καμπύλης γ δίνεται από την

$$P = \int_a^b \sqrt{[x'(t)]^2 + [y'(t)]^2}\, dt. \tag{3.4.8}$$

Θα ορίσουμε πρώτα μία νέα παραμετρικοποίηση της καμπύλης γ: Θεωρούμε την απεικόνιση $s : [a,b] \to [0,P]$ με

$$s(t) = \int_a^t \sqrt{[x'(u)]^2 + [y'(u)]^2} du. \tag{3.4.9}$$

Η s είναι συνεχής και γνησίως αύξουσα συνάρτηση του t, συνεπώς ορίζεται η αντίστροφή της s^{-1} στο $[0,P]$ και μπορούμε να θεωρήσουμε την καμπύλη $\gamma_1 : [0,P] \to \mathbb{R}^2$ με $\gamma_1(s) = \gamma(t)$ όπου $s = s(t)$. Τότε, αν $x_1(s) = x(t)$ και $y_1(s) = y(t)$ έχουμε

$$\frac{dx_1}{ds} = \frac{dx}{dt}\frac{dt}{ds} = \frac{x'(t)}{\sqrt{[x'(t)]^2 + [y'(t)]^2}} \tag{3.4.10}$$

και

$$\frac{dy_1}{ds} = \frac{dy}{dt}\frac{dt}{ds} = \frac{y'(t)}{\sqrt{[x'(t)]^2 + [y'(t)]^2}}. \tag{3.4.11}$$

Από τις παραπάνω σχέσεις βλέπουμε ότι η γ_1 έχει την ιδιότητα

$$(dx_1/ds)^2 + (dy_1/ds)^2 = 1$$

γιά κάθε t. Εχουμε δηλαδή παραμετρικοποιήσει την καμπύλη *ως προς μήκος τόξου*.

Το εμβαδόν του χωρίου K υπολογίζεται με τη βοήθεια του θεωρήματος του Green: Θεωρούμε τις συναρτήσεις $Q(x,y) = x$ και $P(x,y) = -y$. Αν με γ_1 συμβολίσουμε και την εικόνα της καμπύλης γ_1 (το σύνορο δηλαδή του K), τότε

$$\int_{\gamma_1} P dx + Q dy \;=\; \int_K \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right) dxdy, \tag{3.4.12}$$

και για τις συγκεκριμένες P και Q παίρνουμε

$$A(K) = \frac{1}{2}\int_{\gamma_1} x dy - y dx. \tag{3.4.13}$$

Έπεται ότι

$$A(K) = \frac{1}{2}\int_0^P [x_1(s)y_1'(s) - y_1(s)x_1'(s)]ds \tag{3.4.14}$$

και με ολοκλήρωση κατά παράγοντες παίρνουμε

$$A(K) = \int_0^P x_1(s)y_1'(s)ds. \tag{3.4.15}$$

Θα κάνουμε ακόμα μία αλλαγή μεταβλητής: θέτουμε $2\pi s = P\theta$, οπότε $\theta \in [0,2\pi]$ και αν $\gamma_2(\theta) = \gamma_1(s) = (x_2(\theta), y_2(\theta))$, έχουμε

$$[x_2'(\theta)]^2 + [y_2'(\theta)]^2 = \frac{P^2}{4\pi^2} \tag{3.4.16}$$

για κάθε θ, και

$$A(K) = \int_0^{2\pi} x_2(\theta)y_2'(\theta)d\theta. \tag{3.4.17}$$

Απόδειξη του θεωρήματος. Μπορούμε να υποθέσουμε ότι το σύνορο του K είναι η εικόνα μίας καμπύλης $\gamma_2 : [0,2\pi] \to \mathbb{R}^2$ η οποία ικανοποιεί τις (3.9) και (3.10).

Οι συναρτήσεις $x_2(\theta)$ και $y_2(\theta)$ είναι συνεχείς άρα έχουν σειρές Fourier, και επειδή είναι και παραγωγίσιμες οι σειρές Fourier τους συγκλίνουν σε αυτές:

$$x_2(\theta) = \frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \,\text{συν}\, k\theta + b_k \,\text{ημ}\, k\theta) \tag{3.4.18}$$

και

$$y_2(\theta) = \frac{c_0}{2} + \sum_{k=1}^{\infty} (c_k \,\text{συν}\, k\theta + d_k \,\text{ημ}\, k\theta)\,. \tag{3.4.19}$$

Επειδή οι x_2' και y_2' είναι συνεχείς, έχουν σειρές Fourier

$$x_2'(\theta) \;\sim\; \sum_{k=1}^{\infty} (kb_k \,\text{συν}\, k\theta - ka_k \,\text{ημ}\, k\theta) \tag{3.4.20}$$

και

$$y_2'(\theta) \;\sim\; \sum_{k=1}^{\infty} (kd_k \,\text{συν}\, k\theta - kc_k \,\text{ημ}\, k\theta)\,. \tag{3.4.21}$$

Η ταυτότητα του Parseval μας δίνει

$$\int_0^{2\pi} [x_2'(\theta)]^2 d\theta = \pi \sum_{k=1}^{\infty} k^2(a_k^2 + b_k^2) \tag{3.4.22}$$

και

$$\int_0^{2\pi} [y_2'(\theta)]^2 d\theta = \pi \sum_{k=1}^{\infty} k^2(c_k^2 + d_k^2). \tag{3.4.23}$$

Συνδυάζοντας με την (3.9) παίρνουμε

$$P^2(K) = 2\pi^2 \sum_{k=1}^{\infty} k^2(a_k^2 + b_k^2 + c_k^2 + d_k^2). \tag{3.4.24}$$

Από την άλλη πλευρά, η (3.10) μας δίνει

$$A(K) = \int_0^{2\pi} x_2(\theta) y_2'(\theta) d\theta = \pi \sum_{k=1}^{\infty} k(a_k d_k - b_k c_k). \tag{3.4.25}$$

Αφαιρώντας παίρνουμε:

$$P^2 - 4\pi A = 2\pi^2 \sum_{k=1}^{\infty} \left(k^2(a_k^2 + b_k^2 + c_k^2 + d_k^2) - 2k(a_k d_k - b_k c_k) \right) \tag{3.4.26}$$

$$= 2\pi^2 \sum_{k=1}^{\infty} k[(a_k - d_k)^2 + (b_k + c_k)^2] + 2\pi^2 \sum_{k=2}^{\infty} (k^2 - k) \left(a_k^2 + b_k^2 + c_k^2 + d_k^2 \right) \geq 0.$$

Η ανισότητα λοιπόν ισχύει και μένει να εξετάσουμε πότε μπορεί να ισχύει ισότητα. Από την (3.4.26) είναι φανερό ότι γιά $k \geq 2$ πρέπει να έχουμε $a_k = b_k = c_k = d_k = 0$ (αφού $k^2 - k > 0$ αν $k \geq 2$). Επιπλέον, το πρώτο από τα δύο αθροίσματα πρέπει να μηδενίζεται κι αυτό, άρα $a_1 = d_1$ και $b_1 = -c_1$. Δηλαδή,

$$x_2(\theta) = \frac{a_0}{2} + a_1 \operatorname{συν} \theta + b_1 \operatorname{ημ} \theta$$

και

$$y_2(\theta) = \frac{c_0}{2} - b_1 \operatorname{συν} \theta + a_1 \operatorname{ημ} \theta.$$

Ένας απλός υπολογισμός δείχνει ότι

$$\left(x_2(\theta) - \frac{a_0}{2} \right)^2 + \left(y_2(\theta) - \frac{c_0}{2} \right)^2 = a_1^2 + b_1^2, \tag{3.4.27}$$

δηλαδή η καμπύλη γ_2 περιγράφει κύκλο, και το K είναι δίσκος. □