Οπότε αν $\gamma_n(A) \geq \frac{1}{2}$ $\int_{\mathbb{R}^n} e^{\frac{d(x,A)^2}{4}} d\gamma_n(x) \leq 2$

άρα $\int_{A_t^c} e^{\frac{d(x,A)^2}{4}} d\gamma_n(x) \leq \int_{\mathbb{R}^n} e^{\frac{d(x,A)^2}{4}} d\gamma_n(x)$

άρα $\int_{A_t^c} e^{\frac{d(x,A)^2}{4}} d\gamma_n(x) \geq \int_{A_t^c} e^{\frac{t^2}{4}} d\gamma_n(x) = e^{\frac{t^2}{4}} \gamma_n(A_t^c) \Rightarrow \gamma_n(A_t^c) \leq 2e^{-\frac{t^2}{4}}$

$\Rightarrow \gamma_n(A_t) \geq 1 - 2e^{-\frac{t^2}{4}}$

11/03/2025

Γεωμετρία των Αριθμών

Θεώρημα (Minkowski)
Έστω K κυρτό συμμετρικό σύνολο στον $\mathbb{R}^n$ με $|K| > 2^n$. Τότε υπάρχει $x \in \mathbb{Z}^n \setminus \{0\}$ ώστε $x \in K$

Σχόλια:
1) Το 2^n είναι βέλτιστο. Αν πάρουμε τον ανοιχτό κύβο $(-1,1)^n$ τότε έχει όγκο το 0 μόνο
2) Αν K οριακές τότε αν $|K| \geq 2^n$, τότε $\exists x \in \mathbb{Z}^n \setminus \{0\} : x \in K$
Θεωρούμε τα σύνολα $K_s = (1 + \frac{1}{s})K$, $s = 1, 2, \ldots$ για κάθε $s \geq 1$ έχουμε $|K_s| > 2^n$ άρα $\exists x_s \in \mathbb{Z}^n \setminus \{0\}$ ώστε $x_s \in K_s$. Λόγω συμπάγειας υπάρχει υποακολουθία $x_{s_k} \to x$ και $x \in \bigcap_{s=1}^{\infty} K_s \Rightarrow x \in K$ και x_{s_k} τελικά σταθερή, οπότε $x \in \mathbb{Z}^n \setminus \{0\}$

Λήμμα (Blichfeldt)
Έστω $k \in \mathbb{Z}$ και $A \subseteq \mathbb{R}^n$ μετρήσιμο και υποθέτουμε ότι $|A| > k$. Τότε υπάρχει $x \in \mathbb{R}^n$ ώστε το $A + x$ να περιέχει τουλάχιστον $k+1$ ~~σημεία~~ ακέραια σημεία

Απόδειξη

Έστω $f(x) =$ το πλήθος ακεραίων σημείων στο $A + x$

οπότε $f(x) = \sum_{y \in \mathbb{Z}^n} 1_{A+x}(y)$

$\frac{1}{|A|}\int_A f$ ~ μέση τιμή της f

$$\int_{[0,1]^n} f(x)dx = \int_{[0,1]^n} \sum_{y\in\mathbb{Z}^n} 1_{A+x}(y)\,dx = \sum_{y\in\mathbb{Z}^n} \int_{[0,1]^n} 1_{A+x}(y)dx$$

$$\overset{\text{αλλ. μεταβ.}}{=} \sum_{y\in\mathbb{Z}^n} \int_{y-[0,1]^n} 1_A(t)dt = \int_{\mathbb{R}^n} 1_A(t)dt = |A| > K \leftarrow f \text{ κατά μέση τιμή μεγαλύτερη από } K$$

$x = y - t$

$\Rightarrow \exists x\in[0,1]^n : f(x) > K \Rightarrow f(x) \geq K+1$

οπότε υπάρχει x ώστε $A+x$ να περιέχει τουλάχιστον $K+1$ σημεία

Απόδειξη Θεωρήματος (Minkowski)

Εφαρμόζω το Λήμμα για $A = \frac{K}{2}$, τότε $|A|>1$, άρα $\exists\, p,q\in\mathbb{Z}^n$ και $x\in\mathbb{R}^n$ ώστε: $p\in\frac{K}{2}+x \Rightarrow p = \frac{k_1}{2}+x$

$q\in\frac{K}{2}+x \Rightarrow q = \frac{k_2}{2}+x$

Θεωρώ το $p-q$. Το $p-q\neq 0$ και θέλω να δείξω $p-q\in K$

Έχω $p-q = \frac{k_1-k_2}{2} = \frac{1}{2}\underbrace{k_1}_{\in K} + \frac{1}{2}\underbrace{(-k_2)}_{\in K} \in K$

λόγω συμμετρίας

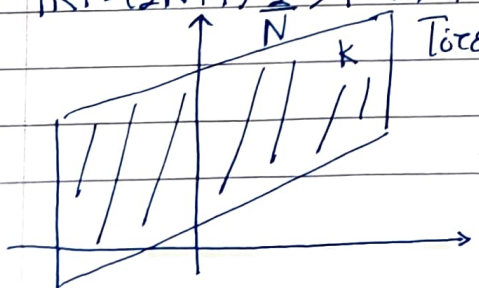
Εφαρμογή 1

Έστω $\alpha\in(0,1)$ και N ένας θετικός ακέραιος. Τότε μπορώ να βρω $m,n\in\mathbb{Z}$ με $0<n\leq N$ ώστε $\left|\alpha - \frac{m}{n}\right| \leq \frac{1}{nN}$

Απόδειξη

Ορίζω το σύνολο $K = \left\{(x,y)\in\mathbb{R}^2 : -N+\frac{1}{2} \leq x \leq N+\frac{1}{2} \text{ και } |\alpha x - y| < \frac{1}{N}\right\}$

$|K| = (2N+1)\cdot\frac{2}{N} > 4$. Από Θ. Minkowski $\exists (m,n)\in(\mathbb{Z}^n\setminus\{0\})\cap K$



Τότε $|\alpha n - m| < \frac{1}{N} \Rightarrow \left|\alpha - \frac{m}{n}\right| < \frac{1}{N\cdot n}$ και $n\neq 0$

γιατί αν $n=0$

τότε $|m| < \frac{1}{N} \Rightarrow m = 0$ άτοπο αφού $(m,n)\neq(0,0)$

Θεώρημα (Lagrange)
Κάθε αριθμός γράφεται ως άθροισμα τεσσάρων τετραγώνων

Σχόλια:
1) Κάθε αριθμός που δεν είναι της μορφής $4^k(8m+7)$ γράφεται ως άθροισμα τριών τετραγώνων
2) Αν ένας αριθμός δεν έχει πρώτο διαιρέτη της μορφής $4k+3$ σε περιττή δύναμη γράφεται ως άθροισμα δύο τετραγώνων

Απόδειξη Θεωρήματος

Παρατήρηση: Αρκεί να αποδείξω το θεώρημα όταν ο n είναι της μορφής $n=p_1\cdots p_s$. Σταθερά μία $n=p_1\cdots p_s$

Λήμμα 1: Αν p πρώτος $\exists a,b$ ώστε $p \mid a^2+b^2+1$

Απόδ

Αν $p=2$ προφανές. Αν p περιττός, αν $0 \le a \le \frac{p-1}{2}$, τότε αυτοί έχουν διαφορετικά τετράγωνα $\bmod p$
Αν $a_1^2 \equiv a_2^2 \pmod p \Leftrightarrow (a_1-a_2)(a_1+a_2) \equiv 0 \pmod p \Rightarrow p \mid a_1+a_2$ ή $p \mid a_1-a_2$
$\le p-1 \quad \Rightarrow a_1=a_2$

Ομοίως αν $0 \le b \le \frac{p-1}{2}$ τα b^2 παίρνουν διαφορετικές τιμές $\bmod p$
Άρα $\exists a,b$: ~~$a^2 \equiv$~~ $a^2 \equiv -b^2-1$ αφού τα a, b είναι $p+1$ το πλήθος
$\left(\frac{p+1}{2} \text{ τιμές}\right) \quad \left(\frac{p+1}{2} \text{ τιμές}\right)$

Λήμμα 2: Αν $n=p_1\cdots p_s$ τότε $\exists a,b: n \mid a^2+b^2+1$
Θέλω να βρω a,b: $a^2+b^2+1 \equiv 0 \pmod{p_1}$
$a^2+b^2+1 \equiv 0 \pmod{p_2}$
$\vdots$
$a^2+b^2+1 \equiv 0 \pmod{p_s}$

Κινέζικο Θεώρημα Υπολοίπων

Απόδειξη Θεωρήματος

Θεωρούμε το γραμμικό μετασχηματισμό $T: \mathbb{R}^4 \to \mathbb{R}^4$ με
$T(e_1) = (1,0,a,-b)$, $T(e_2) = (0,1,b,a)$
$T(e_3) = (a,0,n,0)$, $T(e_4) = (0,0,0,n)$

Ο T είναι αντιστρέψιμος και $\det(T) = n^2$
Αν $u = (u_1, u_2, u_3, u_4) \in \mathbb{Z}^4$ τότε ~~$T(u) = (u_1, u_2, au_1 + bu_2, -bu_1 + au_2)$~~

$T(u) = (u_1, u_2, au_1 + bu_2 + nu_3, -bu_1 + au_2 + nu_4)$

Έστω $B = \{x : x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n\}$

$|B| = 2n^2\pi^2 > 2^4 |\det T| \Rightarrow |T^{-1}(B)| > 2^4$

Από Θ. Minkowski υπάρχει $(u_1, u_2, u_3, u_4) \in T^{-1}(B) \cap \mathbb{Z}^n \setminus \{0\}$

$T(u) \in B \Rightarrow 0 < u_1^2 + u_2^2 + (au_1 + bu_2 + nu_3)^2 + (-bu_1 + au_2 + nu_4)^2 < 2n$

$\equiv u_1^2 + u_2^2 + (au_1 + bu_2)^2 + (-bu_1 + au_2)^2 \pmod n$

$\equiv u_1^2 + u_2^2 + (a^2 + b^2)(u_1^2 + u_2^2) \pmod n$ Ταυτότητα Lagrange

$\equiv (u_1^2 + u_2^2)(a^2 + b^2 + 1) \equiv 0 \pmod n$

και άρα $n = u_1^2 + u_2^2 + (au_1 + bu_2 + nu_3)^2 + (-bu_1 + au_2 + nu_4)^2 < 2n$

14/03/2025

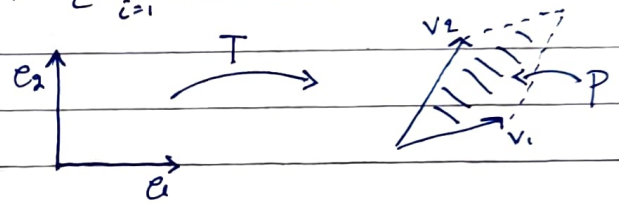
Ακέραια σημεία σε ελλειψοειδή

Ένα ελλειψοειδές E είναι μια γραμμική εικόνα της μοναδιαίας B_2^n. Δηλ $E = T(B_2^n)$
Μπορεί να οριστεί το ελλειψοειδή στη μορφή $E = \{x \in \mathbb{R}^n : \sum_{i=1}^{n} \frac{x_i^2}{a_i^2} \leq 1\}$

Θεώρημα (Blichfeldt)
Αν E είναι ελλειψοειδές με $|E| > 2^{\frac{n}{2}}(\frac{n+2}{2})$, τότε το E έχει ακέραιο σημείο εκτός το 0

Απόδειξη ← πλέγμα (Lattice)
Αρκεί ισοδύναμα να δω αν $\Lambda = T(\mathbb{Z}^n)$ για κάποιο γραμμικό T και $|B_2^n| > 2^{\frac{n}{2}}(\frac{n+2}{2})|\det T|$ τότε $\exists x \in B_2^n \cap (\Lambda \setminus \{0\})$

Αν $v_i = T(e_i)$ τότε ορίζεται το $P = \{\sum_{i=1}^{n} t_i v_i : 0 \leq t_i \leq 1\}$
(Το παραλληλόγραμμο)



Τότε $|P| = |\det T|$

Για κάθε ολοκληρώσιμη $f: \mathbb{R}^n \to \mathbb{R}$ ισχύει ότι:

$$\int_{\mathbb{R}^n} f(x)dx = \sum_{u \in \Lambda} \int_{u+P} f(x)dx \overset{\text{αλλ. μετ.}}{\underset{x=u+y}{=}} \sum_{u \in \Lambda} \int_P f(u+y)dy = \int_P \sum_{u \in \Lambda} f(u+y)dy$$

Αν έχω f τέτοια ώστε $\int_{\mathbb{R}^n} f(x)dx > |P|$

τότε $\frac{1}{|P|} \int_P \sum_{u \in \Lambda} f(u+y)dy > 1$ οπότε $\exists y \in P : \sum_{u \in \Lambda} f(u+y) > 1$

Ισχυρισμός: Μια τέτοια συνάρτηση με αυτήν την ιδιότητα είναι η
$f(x) = \begin{cases} 1 - 2\|x\|_2^2, & \text{αν } \|x\|_2 \leq 1/\sqrt{2} \\ 0, & \text{αλλιώς} \end{cases}$

Απόδειξη Ισχυρισμού

$$\int_{\mathbb{R}^n} f(x)\,dx = \int_{\frac{1}{\sqrt{2}}B_2^n} (1-2\|x\|_2^2)\,dx = \int_{rB_2^n} \left(1-\frac{\|x\|_2^2}{r^2}\right)dx \quad \text{όπου } r=\frac{1}{\sqrt{2}}$$

(Μπορείς να χάνεις αλλαγή σε πολικές συντεταγμένες στον $\mathbb{R}^n$)

$$\int_{\mathbb{R}^n} f(x)\,dx = \int_0^\infty \int_{S^{n-1}} f(r\theta)\, r^{n-1}\, d\theta\, dr$$

$$\int_{rB_2^n} \left(1-\frac{\|x\|_2^2}{r^2}\right)dx = |rB_2^n| - \frac{1}{r^2}\int_{rB_2^n} \|x\|_2^2\,dx = |rB_2^n| - \frac{1}{r^2}\int_{rB_2^n}\int_0^{\|x\|_2} 2t\,dt\,dx$$

$$= |rB_2^n| - \frac{1}{r^2}\int_{rB_2^n}\int_0^r 2t\,\mathbb{1}_{\{t\le\|x\|_2\le r\}}\,dt\,dx$$

$$= |rB_2^n| - \frac{1}{r^2}\int_0^r 2t\left(|rB_2^n| - |tB_2^n|\right)dt = \frac{2}{2n+2}|rB_2^n| \overset{r=\frac{1}{\sqrt{2}}}{=}$$

$$= \boxed{\frac{2}{n+2}\cdot\frac{1}{2^{\frac{n}{2}}}|B_2^n|} \overset{\text{γνωστό}}{>} |\det T| = |P|$$

Επομένως $\exists y\in\mathbb{R}^n : \sum_{u\in\Lambda}(1-2\|u+y\|_2^2) > 1$ (*) $\quad\left(\|u+y\|_2 \le \frac{1}{\sqrt{2}}\right)$

Αυτό ισχύει για περιορισμένα σύνολα του Λ, έστω $u_1,\dots,u_m$

τότε (*) $\Rightarrow \sum_{i=1}^m (1-2\|u_i+y\|_2^2) > 1 \Rightarrow \sum_{i=1}^m \|u_i+y\|_2^2 < \frac{m-1}{2}$ (**)

Λήμμα: Αν $y,u_1,\dots,u_m\in\mathbb{R}^n$ τότε $\sum_{i=1}^m\sum_{j=1}^m \|u_i-u_j\|_2^2 \le 2m\sum_{i=1}^m \|u_i+y\|_2^2$

Απόδ

Θέτω $v_i = u_i + y$. Τότε θέλω $A = \sum_{i=1}^m\sum_{j=1}^m \|v_i-v_j\|_2^2 \le 2m\sum_{i=1}^m \|v_i\|_2^2$

$$A = \sum_{i=1}^m\sum_{j=1}^m \left(\|v_i\|_2^2 + \|v_j\|_2^2 - 2\langle v_i, v_j\rangle\right)$$

$$= 2m\sum_{i=1}^m \|v_i\|_2^2 - 2\sum_{i=1}^m \left\langle v_i, \sum_{j=1}^m v_j\right\rangle = 2m\sum_{i=1}^m \|v_i\|_2^2 - 2\left\|\sum_{i=1}^m v_i\right\|_2^2$$

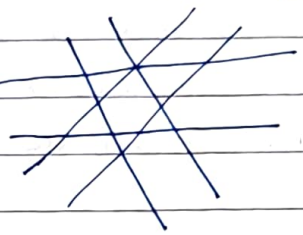
Από το Λήμμα και την (**)

$$\sum_{i=1}^{m}\sum_{j=1}^{m}\|u_i-u_j\|_2^2 < m(m-1) \Rightarrow \exists\, i,j : \|\underbrace{u_i-u_j}_{v}\|_2 < 1 \Rightarrow v\in\Lambda\cap B_2^n \text{ και } v\neq 0$$

Μπορούμε να βρούμε ελλειψοειδές με όγκο $=2(n-1)$ χωρίς ακέραιο σημείο

Λήμμα (Bang)
Αν $x_1,\dots,x_m\in S^{n-1}$ και $w_1,\dots,w_m$ θετ. πραγματικοί αριθμοί, τότε υπάρχει επιλογή προσήμων $\varepsilon_1,\dots,\varepsilon_m\in\{-1,1\}$ ώστε για το διανύσμα $u=\sum_{i=1}^{m}\varepsilon_i w_i x_i$ να ισχύει $|\langle u,x_i\rangle|\geq w_i$ $\forall\, i=1,2,\dots,m$

$|\langle y,x_i\rangle|\leq w_i$



Απόδειξη
Για κάθε $\varepsilon=(\varepsilon_1,\dots,\varepsilon_m)\in\{-1,1\}^m$ ορίζω $u(\varepsilon)=\sum_{i=1}^{m}\varepsilon_i x_i w_i$

Από όλα αυτά τα διανύσματα επιλέγω αυτό με το μεγαλύτερο μήκος έστω $u(\varepsilon^*)$
Ορίζουμε το διανύσμα u_j με $u_j=u(\varepsilon^*)-2\varepsilon_j^* x_j w_j$

$$\|u(\varepsilon^*)\|_2^2 \geq \|u_j\|_2^2 = \|u(\varepsilon^*)-2\varepsilon_j^* x_j w_j\|_2^2$$
$$= \|u(\varepsilon^*)\|_2^2 - 4\varepsilon_j^* w_j\langle u(\varepsilon^*),x_j\rangle + 4w_j^2$$

$$\Rightarrow \varepsilon_j^*\langle u(\varepsilon^*),x_j\rangle \geq w_j \Rightarrow$$

$$|\langle u(\varepsilon^*),x_j\rangle| \geq \varepsilon_j^*\langle u(\varepsilon^*),x_j\rangle \geq w_j$$