GEOMETRY OF NUMBERS C

Tapani Matala-aho, Aalto University, 2022

The first Minkowski's convex body theorem

The first Minkowski's convex body theorem. Let $n \in \mathbb{Z}^+$. Assume that $\Lambda \subseteq \mathbb{R}^n$ is a lattice with rank $\Lambda = n$ and $\mathcal{C} \subseteq \mathbb{R}^n$ is a central symmetric convex body with

$$\operatorname{vol} \mathcal{C} > 2^n \det \Lambda \quad \text{or}$$

$$\operatorname{vol} \mathcal{C} \geq 2^n \det \Lambda, \quad \text{if} \quad \mathcal{C} \quad \text{is compact.}$$

Then, there exists a non-zero lattice point in $\mathcal{C}$. In fact, then $\#\mathcal{C} \cap \Lambda \geq 3$.

Theorem of Blichfeldt

First we prove Blichfeldt's theorem.

Theorem 1

Blichfeldt. Let $n \in \mathbb{Z}^+$. *Assume that a subset* $\mathcal{R} \subseteq \mathbb{R}^n$ *and a full lattice* $\Lambda \subseteq \mathbb{R}^n$ *are such that*

$$\infty > \operatorname{vol} \mathcal{R} > \det \Lambda. \tag{1}$$

Then there exist points $\overline{r}_1, \overline{r}_2 \in \mathcal{R}$, $\overline{r}_1 \neq \overline{r}_2$, *satisfying*

$$\overline{r}_1 - \overline{r}_2 \in \Lambda. \tag{2}$$

Theorem of Blichfeldt

Proof. Recall the notation of the fundamental domain

$$\mathcal{F} = \mathcal{F}(\bar{l}_1, \ldots, \bar{l}_n) := \{x_1\bar{l}_1 + \ldots + x_n\bar{l}_n \mid 0 \leq x_i < 1\} \tag{3}$$

and its translates

$$\mathcal{F}_j := \overline{h}_j + \mathcal{F} \tag{4}$$

with the fact that every $\overline{x} \in \mathbb{R}^n$ has a unique representation

$$\overline{x} = \overline{h}_j + \overline{f}, \quad \overline{h}_j \in \Lambda, \ \overline{f} \in \mathcal{F}. \tag{5}$$

Then, for $\overline{h}_j \in \Lambda$ we set

$$\mathcal{R}_j = \mathcal{R}(\overline{h}_j) := \mathcal{R} \cap \mathcal{F}_j. \tag{6}$$

Theorem of Blichfeldt

It follows that

$$\sqcup \mathcal{R}_j = \mathcal{R}, \tag{7}$$

a disjoint union. In other words, our domain $\mathcal{R}$ is divided into disjoint translates of the fundamental domain. Now we define translates

$$\mathcal{T}_j := \mathcal{R}_j - \overline{h}_j \subseteq \mathcal{F}, \tag{8}$$

which are pullbacks into the fundamental domain satisfying

$$\operatorname{vol} \mathcal{T}_j = \operatorname{vol} \mathcal{R}_j. \tag{9}$$

Theorem of Blichfeldt

Hence

$$\sum \operatorname{vol} \mathcal{T}_j = \sum \operatorname{vol} \mathcal{R}_j = \operatorname{vol} \mathcal{R} \overset{(1)}{>} \det(\Lambda) = \operatorname{vol} \mathcal{F}. \tag{10}$$

But

$$\cup \mathcal{T}_j \subseteq \mathcal{F}. \tag{11}$$

Therefore, there exist, say $\mathcal{T}_1$ and $\mathcal{T}_2$, which overlap. Take a

$$\overline{f}_0 \in \mathcal{T}_1 \cap \mathcal{T}_2. \tag{12}$$

Theorem of Blichfeldt

Thus

$$\begin{aligned} \overline{f}_0 &= \overline{r}_1 - \overline{h}_1, \quad \overline{r}_1 \in \mathcal{R}_1, \quad \overline{h}_1 \in \Lambda; \\ \overline{f}_0 &= \overline{r}_2 - \overline{h}_2, \quad \overline{r}_2 \in \mathcal{R}_2, \quad \overline{h}_2 \in \Lambda, \end{aligned} \tag{13}$$

where

$$\mathcal{R}_1 \cap \mathcal{R}_2 = \emptyset. \tag{14}$$

Hence

$$\begin{aligned} \overline{r}_1 \neq \overline{r}_2 \quad \text{and} \\ \overline{r}_1 - \overline{r}_2 = \overline{h}_1 - \overline{h}_2 \in \Lambda. \quad \square \end{aligned} \tag{15}$$

The first Minkowski's convex body theorem/Non-compact version

Theorem 2

The first Minkowski's convex body theorem. Let $n \in \mathbb{Z}^+$. Assume that $\Lambda \subseteq \mathbb{R}^n$ is a lattice with rank $\Lambda = n$ and $\mathcal{C} \subseteq \mathbb{R}^n$ is a central symmetric convex body with

$$\operatorname{vol} \mathcal{C} > 2^n \det \Lambda. \tag{16}$$

Then, there exists a non-zero lattice point in $\mathcal{C}$.

The first Minkowski's convex body theorem

Proof. Consider the volume of the dilation

$$\operatorname{vol}\frac{1}{2}\mathcal{C} = \frac{1}{2^n}\operatorname{vol}\mathcal{C} \overset{(16)}{>} \det\Lambda. \tag{17}$$

By Theorem 1 there exist disjoint points $\overline{r}_1, \overline{r}_2 \in \frac{1}{2}\mathcal{C}$ such that $\overline{x} := \overline{r}_1 - \overline{r}_2 \in \Lambda \setminus \{\overline{0}\}$. The assumption $-\mathcal{C} = \mathcal{C}$ implies $-\overline{r}_2 \in \frac{1}{2}\mathcal{C}$. Thus we have $2\overline{r}_1, -2\overline{r}_2 \in \mathcal{C}$. Therefore, by convexity

$$\frac{1}{2}(2\overline{r}_1) + \frac{1}{2}(-2\overline{r}_2) = \overline{r}_1 - \overline{r}_2 = \overline{x} \in \mathcal{C}. \tag{18}$$

Hence there exists a non-zero vector

$$\overline{x} \in \mathcal{C} \cap \Lambda. \quad \square \tag{19}$$

Undressed Minkowski

In particular, if Λ is the integer lattice $\mathbb{Z}^n$, then we have the following handy version for a bunch of cases.

Theorem 3

If $\mathcal{B} \subseteq \mathbb{R}^n$ is a central symmetric convex body such that

$$\operatorname{vol} \mathcal{B} > 2^n, \tag{20}$$

then

$$\mathcal{B} \cap \mathbb{Z}^n \neq \{\bar{0}\}. \tag{21}$$

Undressed Minkowski/Compact case

Next we will prove a compact version of Theorem 3.

Theorem 4

If $\mathcal{B} \subseteq \mathbb{R}^n$ *is a compact central symmetric convex body such that*

$$\operatorname{vol} \mathcal{B} \geq 2^n, \tag{22}$$

then

$$\mathcal{B} \cap \mathbb{Z}^n \neq \{\overline{0}\}. \tag{23}$$

Undressed Minkowski/Compact case

Proof. Now we may suppose $\operatorname{vol}\mathcal{B} = 2^n$. Suppose on the contrary that $\mathcal{B}$ does not contain a non-zero point from $\mathbb{Z}^n$.

Because the set $\mathcal{B}$ is compact, the maximum $M_1 := \max\{\|\overline{x}\|_2 \mid \overline{x} \in \mathcal{B}\}$ exists. Now we write $M := \lceil M_1 \rceil + 1$ and define an n-cube

$$\square(S) := \{(x_1, \ldots, x_n) \in S^n \mid |x_i| \leq M,\ \ i = 1, \ldots n\} \tag{24}$$

in $\mathbb{R}^n$. First we see $\mathcal{B} \subseteq \square(\mathbb{R})$.

Undressed Minkowski/Compact case

Consequently, there are only finitely many lattice points outside $\mathcal{B}$ but inside $\square(\mathbb{Z})$ or

$$\# \square(\mathbb{Z}) \setminus \mathcal{B} < \infty. \tag{25}$$

Since $\mathcal{B}$ is compact and $\square(\mathbb{Z}) \setminus \mathcal{B}$ is finite, there exists a $b > 1$ such that $b\mathcal{B} \subseteq \square(\mathbb{R})$ and $b\mathcal{B} \cap \square(\mathbb{Z})$ does not contain a non-zero point. But

$$\operatorname{vol} b\mathcal{B} = b^n \operatorname{vol} \mathcal{B} > 2^n, \tag{26}$$

which yields to a contradiction. □

Minkowski/Compact body version

Theorem 5

The first Minkowski's convex body theorem. Let $n \in \mathbb{Z}^+$. Assume that $\Lambda \subseteq \mathbb{R}^n$ is a lattice with rank $\Lambda = n$ and $\mathcal{C} \subseteq \mathbb{R}^n$ is a compact central symmetric convex body with

$$\operatorname{vol} \mathcal{C} \geq 2^n \det \Lambda, \tag{27}$$

then

$$\mathcal{C} \cap \Lambda \neq \{\overline{0}\}. \tag{28}$$

Minkowski/Compact body version

Proof. Let L be the linear map defined by the lattice Λ. Because $\Lambda = L\mathbb{Z}^n$ is a full lattice, then $L : \mathbb{R}^n \to \mathbb{R}^n$ is a bijection and $\det \Lambda = |\det L|$. The set $\mathcal{B} := L^{-1}\mathcal{C}$ is a compact central symmetric convex body and its volume satisfies the inequality

$$\operatorname{vol} \mathcal{B} = \left| \det L^{-1} \right| \cdot \operatorname{vol} \mathcal{C} \geq \frac{1}{|\det L|} \cdot 2^n \det \Lambda = 2^n. \tag{29}$$

Therefore there exists an $\overline{x} \neq \overline{0}$ such that

$$\overline{x} \in \mathcal{B} \cap \mathbb{Z}^n. \tag{30}$$

Further, $L\overline{x} \neq \overline{0}$ and

$$L\overline{x} \in \mathcal{C} \cap \Lambda. \quad \square \tag{31}$$

Minkowski/Linear map version

Corollary 6

Let $L: \mathbb{R}^n \to \mathbb{R}^n$ *be a one to one linear transformation. Assume* $\mathcal{B} \subseteq \mathbb{R}^n$ *is a central symmetric convex body such that*

$$\operatorname{vol} \mathcal{B} > 2^n \quad \text{or}$$

$$\operatorname{vol} \mathcal{B} \geq 2^n, \quad \text{if} \quad \mathcal{B} \quad \text{is compact.}$$

Then

$$\mathcal{C} \cap \Lambda \tag{32}$$

contains a non-zero point, where $\mathcal{C} := L\mathcal{B}$ *and* $\Lambda := L(\mathbb{Z}^n)$.

Minkowski/Linear map version

Proof. All we need to know is

$$\operatorname{vol}\mathcal{C} = \operatorname{vol} L\mathcal{B} = |\det L| \operatorname{vol}\mathcal{B} \begin{cases} > 2^n \det\Lambda, \\ \geq 2^n \det\Lambda, \quad \mathcal{B} \text{ compact.} \end{cases} \tag{33}$$

Thus $\mathcal{C} \cap \Lambda = L\mathcal{B} \cap L(\mathbb{Z}^n)$ contains a non-zero point. □

A Diophantine equation

Prove that the Diophantine equation

$$2x^2 + 10xy + 13y^2 = 1 \tag{34}$$

has a non-trivial solution $(x, y) \in \mathbb{Z}^2$. Define

$$\mathcal{E} := \{\overline{x} \in \mathbb{R}^2 \mid 2x^2 + 10xy + 13y^2 < 2\}, \quad \Lambda = \mathbb{Z}^2. \tag{35}$$

Note, that

$$\mathcal{E} = \{\overline{x} \in \mathbb{R}^2 \mid (2x+5y)^2+y^2 < 4\} = \left\{\overline{x} \in \mathbb{R}^2 \,\middle|\, \left(x + \frac{5}{2}y\right)^2 + \left(\frac{y}{2}\right)^2 < 1\right\} \tag{36}$$

A Diophantine equation

Define a linear map by setting

$$L\overline{x} = L(x,y) := (x + \frac{5}{2}y, \frac{y}{2}). \tag{37}$$

It holds

$$L = \begin{bmatrix} 1 & \frac{5}{2} \\ 0 & \frac{1}{2} \end{bmatrix}, \quad \det L = \frac{1}{2}. \tag{38}$$

Therefore L is bijective. Using (36) we see that

$$L\mathcal{E} = \{(\alpha,\beta) \in \mathbb{R}^2 \mid \alpha^2 + \beta^2 < 1,\ (\alpha,\beta) = L\overline{x},\ \overline{x} \in \mathbb{R}^2\}. \tag{39}$$

A Diophantine equation

Write

$$\mathcal{D} := \{(A, B) \in \mathbb{R}^2 \mid A^2 + B^2 < 1\}. \tag{40}$$

By surjectivity of L we have

$$\mathcal{D} = L\mathcal{E}. \tag{41}$$

A Diophantine equation

Because

$$\pi = \operatorname{vol} \mathcal{D} = \det L \cdot \operatorname{vol} \mathcal{E} = \frac{1}{2} \operatorname{vol} \mathcal{E} \tag{42}$$

we get

$$\operatorname{vol} \mathcal{E} = 2\pi > 2^2 \det \Lambda = 4. \tag{43}$$

In addition $\mathcal{E}$ is a central symmetric convex body. Therefore, $\mathcal{E} \cap \mathbb{Z}^2$ contains a non-zero point, say $(a, b) \in \mathbb{Z}^2$, meaning

$$0 < 2a^2 + 10ab + 13b^2 < 2 \quad \Rightarrow \quad 2a^2 + 10ab + 13b^2 = 1. \quad \square \tag{44}$$

Linear forms/Compact version

Theorem 7

Let

$$L_i\overline{x} := \alpha_{i1}x_1 + ... + \alpha_{iN}x_N, \quad i = 1, \ldots, N$$

be homogeneous linearly independent linear forms with $\alpha_{ij} \in \mathbb{R}$. *Assume*

$$\tau_1, ..., \tau_N \in \mathbb{R}^+, \quad |\det L| \leq \tau_1 \cdots \tau_N. \tag{45}$$

Then there exists a $\overline{q} \in \mathbb{Z}^N \setminus \{\overline{0}\}$ *such that*

$$|L_i\overline{q}| \leq \tau_i \quad \forall\ i = 1, \ldots, N. \tag{46}$$

Linear forms

Proof. Define a linear map

$$L := (L_1, L_2, \dots, L_N)^T, \tag{47}$$

$$L\overline{x} := \begin{bmatrix} L_1\overline{x} \\ L_2\overline{x} \\ \vdots \\ L_N\overline{x} \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \dots & \alpha_{1N} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \dots & \alpha_{2N} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \dots & \alpha_{3N} \\ . & . & . & \dots & . \\ \alpha_{N1} & \alpha_{N2} & \alpha_{N3} & \dots & \alpha_{NN} \end{bmatrix} \overline{x} \tag{48}$$

By the linear independence of the linear forms follows $\det L \neq 0$. Hence $L : \mathbb{R}^N \to \mathbb{R}^N$ is bijective.

Linear forms

We have $\Lambda := L(\mathbb{Z}^N)$ and $\det\Lambda = |\det L| \neq 0$. Therefore Λ is a full lattice. Further,

$$\Lambda = L(\mathbb{Z}^N) = \mathbb{Z}\bar{\ell}_1 + \mathbb{Z}\bar{\ell}_2 + \ldots + \mathbb{Z}\bar{\ell}_N$$
$$= \mathbb{Z}\begin{bmatrix}\alpha_{11}\\ \alpha_{21}\\ \alpha_{31}\\ \vdots\\ \alpha_{N1}\end{bmatrix} + \mathbb{Z}\begin{bmatrix}\alpha_{12}\\ \alpha_{22}\\ \alpha_{32}\\ \vdots\\ \alpha_{N2}\end{bmatrix} + \ldots + \mathbb{Z}\begin{bmatrix}\alpha_{1N}\\ \alpha_{2N}\\ \alpha_{3N}\\ \vdots\\ \alpha_{NN}\end{bmatrix}. \tag{49}$$

Linear forms

Define sets $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{T}$ by setting

$$\begin{aligned} \mathcal{B} &:= \left\{ \overline{x} \in \mathbb{R}^N \,\middle|\, |L_i\overline{x}| \le \tau_i,\ i = 1, \ldots, N \right\}, \\ \mathcal{C} &:= L\mathcal{B} = \left\{ L\overline{x} \,\middle|\, \overline{x} \in \mathcal{B} \right\}, \\ \mathcal{T} &:= \left\{ \overline{z} \in \mathbb{R}^N \,\middle|\, |z_i| \le \tau_i,\ i = 1, \ldots, N \right\}. \end{aligned} \tag{50}$$

Let us prove that $\mathcal{C} = \mathcal{T}$. First we show that $\mathcal{C} \subseteq \mathcal{T}$. Take a $\overline{w} \in \mathcal{C}$. Then there exists an $\overline{x} \in \mathcal{B}$ such that $\overline{w} = (w_1, \ldots, w_N) = L\overline{x} = (L_1\overline{x}, \ldots, L_N\overline{x})$ and $|w_i| = |L_i\overline{x}| \le \tau_i$, $i = 1, \ldots, N$. Thus $\overline{w} \in \mathcal{T}$. Next we show $\mathcal{T} \subseteq \mathcal{C}$. Take a $\overline{z} \in \mathcal{T}$. Because L is surjective there exists an $\overline{x} \in \mathbb{R}^N$ such that $\overline{z} = (z_1, \ldots, z_N) = L\overline{x} = (L_1\overline{x}, \ldots, L_N\overline{x})$. Hereby $|L_i\overline{x}| = |z_i| \le \tau_i$, which shows that $\overline{x} \in \mathcal{B}$. Consequently $\overline{z} = L\overline{x} \in L\mathcal{B} = \mathcal{C}$.

Linear forms

The volume of the orthotope $\mathcal{T}$ is given by

$$\operatorname{vol}\mathcal{T} = 2^N \tau_1 \cdots \tau_N. \tag{51}$$

On the other hand $\operatorname{vol}\mathcal{C} = |\det L| \operatorname{vol}\mathcal{B}$. Thereby

$$\operatorname{vol}\mathcal{B} = \frac{\operatorname{vol}\mathcal{C}}{|\det L|} = \frac{\operatorname{vol}\mathcal{T}}{|\det L|} \geq \frac{2^N \tau_1 \cdots \tau_N}{\tau_1 \cdots \tau_N} = 2^N. \tag{52}$$

In addition, because the set $\mathcal{T}$ is a compact central symmetric convex body, so is $\mathcal{B} = L^{-1}\mathcal{T}$, too.

Linear forms

Thus $\mathcal{B} \cap \mathbb{Z}^N$ contains a non-zero point, say $\overline{q} = (q_1, \ldots, q_N)$, and therefore $\mathcal{C} \cap \Lambda = L\mathcal{B} \cap L(\mathbb{Z}^N)$ contains a non-zero point $L\overline{q}$. Hence there exists a $\overline{q} \in \mathbb{Z}^N \setminus \{\overline{0}\}$ such that

$$|L_i\overline{q}| \leq \tau_i \quad \forall\ i = 1, \ldots, N. \quad \square \tag{53}$$

Linear forms/Two alternative final conclusions

1. From the fact

$$\overline{q} \in \mathcal{B} = \left\{ \overline{x} \in \mathbb{R}^N \,\middle|\, |\alpha_{i1}x_1 + \ldots + \alpha_{iN}x_N| \leq \tau_i,\ i = 1, \ldots, N \right\} \tag{54}$$

we may deduce that

$$|\alpha_{i1}q_1 + \ldots + \alpha_{iN}q_N| \leq \tau_i \quad \forall\ i = 1, \ldots, N. \quad \square \tag{55}$$

2. From the fact

$$L\overline{q} \in \mathcal{C} = \left\{ L\overline{x} \,\middle|\, |L_i\overline{x}| \leq \tau_i,\ i = 1, \ldots, N \right\} \tag{56}$$

we may deduce again that

$$|L_i\overline{q}| = |\alpha_{i1}q_1 + \ldots + \alpha_{iN}q_N| \leq \tau_i \quad \forall\ i = 1, \ldots, N. \quad \square \tag{57}$$

Linear forms/Non-compact version

Theorem 8

Let

$$L_i\overline{x} := \alpha_{i1}x_1 + ... + \alpha_{iN}x_N, \quad i = 1, \ldots, N$$

be homogeneous linearly independent linear forms with $\alpha_{ij} \in \mathbb{R}$. *Assume*

$$\tau_1, ..., \tau_N \in \mathbb{R}^+, \quad |\det L| < \tau_1 \cdots \tau_N. \tag{58}$$

Then there exists a $\overline{q} \in \mathbb{Z}^N \setminus \{\overline{0}\}$ *such that*

$$|L_i\overline{q}| < \tau_i \quad \forall i = 1, \ldots, N. \tag{59}$$

Circular disk example (problem 18)

Example 1

Let α_1 and α_2 be real numbers and n a positive integer. Prove that there are integers p_1, p_2, q such that

$$1 \leq q \leq n \tag{60}$$

and

$$\left(\alpha_1 - \frac{p_1}{q}\right)^2 + \left(\alpha_2 - \frac{p_2}{q}\right)^2 \leq \frac{4}{\pi n q^2}. \tag{61}$$

First we note, that $q \neq 0$ in (61).

Circular disk example

Proof. If $q \neq 0$, then inequality (61) is equivalent to

$$(q\alpha_1 - p_1)^2 + (q\alpha_2 - p_2)^2 \leq \frac{4}{\pi n} =: R^2. \tag{62}$$

Next we replace q, p_1, p_2 by real numbers x_0, x_1, x_2 and define a set

$$\mathcal{B} := \left\{(x_0, x_1, x_2) \in \mathbb{R}^3 \;\middle|\; |x_0| \leq n,\ (x_0\alpha_1 - x_1)^2 + (x_0\alpha_2 - x_2)^2 \leq R^2\right\}, \tag{63}$$

where the bound $|x_0| \leq n$ is chosen instead of (60) to build a central symmetric body $\mathcal{B}$.

Circular disk example

Write $\overline{x} := (x_0, x_1, x_2)^t$. Then

$$\mathcal{B} = \left\{ \overline{x} \in \mathbb{R}^3 \,\middle|\, |L_0\overline{x}| \leq n,\ (L_1\overline{x})^2 + (L_2\overline{x})^2 \leq R^2 \right\}, \tag{64}$$

where

$$L\overline{x} := \begin{bmatrix} L_0\overline{x} \\ L_1\overline{x} \\ L_2\overline{x} \end{bmatrix} = \begin{bmatrix} x_0 \\ x_0\alpha_1 - x_1 \\ x_0\alpha_2 - x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ \alpha_1 & -1 & 0 \\ \alpha_2 & 0 & -1 \end{bmatrix} \overline{x}. \tag{65}$$

Because $\det L = 1$, then $L : \mathbb{R}^3 \to \mathbb{R}^3$ is bijective.

Circular disk example

We define a corresponding lattice by $\Lambda := L(\mathbb{Z}^3)$. Consequently $\det \Lambda = |\det L| = 1$. Therefore Λ is a full lattice. Further,

$$\begin{aligned} \Lambda = L(\mathbb{Z}^3) &= \mathbb{Z}\bar{\ell}_1 + \mathbb{Z}\bar{\ell}_2 + \mathbb{Z}\bar{\ell}_3 \\ &= \mathbb{Z}\begin{bmatrix} 1 \\ \alpha_1 \\ \alpha_2 \end{bmatrix} + \mathbb{Z}\begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix} + \ldots + \mathbb{Z}\begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}. \end{aligned} \tag{66}$$

Circular disk example

Define sets $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{T}$ by setting

$$\begin{aligned} \mathcal{B} &= \left\{\overline{x} \in \mathbb{R}^3 \,\middle|\, |L_0\overline{x}| \leq n,\ (L_1\overline{x})^2 + (L_2\overline{x})^2 \leq R^2\right\}, \\ \mathcal{C} &:= L\mathcal{B} = \left\{L\overline{x} \,\middle|\, \overline{x} \in \mathcal{B}\right\} \\ &= \left\{(L_0\overline{x}, L_1\overline{x}, L_2\overline{x}) \in \mathbb{R}^3 \,\middle|\, |L_0\overline{x}| \leq n,\ (L_1\overline{x})^2 + (L_2\overline{x})^2 \leq R^2\right\}, \\ \mathcal{T} &:= \left\{(z_0, z_1, z_2) \in \mathbb{R}^3 \,\middle|\, |z_0| \leq n,\ (z_1)^2 + (z_2)^2 \leq R^2\right\}. \end{aligned} \tag{67}$$

It can be proved that $\mathcal{C} = \mathcal{T}$ in a similar manner like in the proof of Theorem 7, see the deduction after (50).

Circular disk example

The volume of the circular cylinder $\mathcal{T}$ is given by

$$\operatorname{vol}\mathcal{T} = 2n\pi R^2 = 8. \tag{68}$$

On the other hand

$$\operatorname{vol}\mathcal{T} = \operatorname{vol}\mathcal{C} = |\det L| \operatorname{vol}\mathcal{B} = \operatorname{vol}\mathcal{B}. \tag{69}$$

Thereby

$$\operatorname{vol}\mathcal{B} = 8 = 2^3 \det\Lambda. \tag{70}$$

In addition, because the set $\mathcal{T}$ is a compact central symmetric convex body, so is $\mathcal{B} = L^{-1}\mathcal{T}$, too.

Circular disk example

Thus, by Theorem 4 the intersection $\mathcal{B} \cap \mathbb{Z}^3$ contains a non-zero integer point, say $(q, p_1, p_2) \in \mathbb{Z}^3 \setminus \{\overline{0}\}$. We also have $q \neq 0$. Hence there exists a $(q, p_1, p_2) \in \mathbb{Z}^3 \setminus \{\overline{0}\}$ such that

$$\begin{aligned} &1 \leq |q| \leq n, \\ &(q\alpha_1 - p_1)^2 + (q\alpha_2 - p_2)^2 \leq \frac{4}{\pi n}. \end{aligned} \tag{71}$$

If $q < 0$, then $-q, -p_1, -p_2$ would be a solution. Therefore we may take $q \geq 1$. □