Integer Points in Polyhedra Gennady Shmonin

Minkowski's theorem and its applications

March 3, 2009

1 Characterization of lattices

In this section, we prove that there is another, equivalent definition of lattices: a lattice is a discrete subgroup of $\mathbb{R}^n$, i.e., a set of vectors $\Lambda \subseteq \mathbb{R}^n$ such that

(a) $z \pm z' \in \Lambda$ whenever $z, z' \in \Lambda$, and

(b) there is a ball $\mathscr{B}_\varepsilon := \left\{x \in \mathbb{R}^n : \|x\| \leqslant \varepsilon\right\}$ such that $\mathscr{B}_\varepsilon \cap \Lambda = \{0\}$.

Since all norms in a finite-dimensional space are equivalent up to a constant factor, condition (b) is invariant over different choices of the norm in $\mathbb{R}^n$. For simplicity, for the rest of this section we shall assume that $\|\cdot\|$ denotes the ℓ_2-norm. Yet, condition (b) actually implies that $(z + \mathscr{B}_\varepsilon) \cap \Lambda = \{z\}$ for all vectors $z \in \Lambda$ (since $z' \in (z + \mathscr{B}_\varepsilon) \cap \Lambda$ implies $z' - z \in \Lambda \cap \mathscr{B}_\varepsilon$). The latter can be read as follows: if z and z' are two vectors in Λ and $\|z - z'\| \leqslant \varepsilon$, then $z = z'$. This property turns out to be helpful when, for example, we consider convergent sequences of lattice vectors: if $z_1, z_2, \dots$ is a sequence of vectors in Λ that converges to a vector z, then there is an index i_0 such that $z_i = z$ for all $i \geqslant i_0$, and therefore, z is also a lattice vector.

1.1 Lattices are discrete groups

It is clear that every lattice $\Lambda = \Lambda(B)$ satisfies condition (a) in the definition of a discrete group. There are many ways to check that condition (b) is also true; we present one which will be especially useful for us later. For a basis $B = \left[b_1, b_2, \dots, b_n\right]$ we denote $B^* = \left[b_1^*, b_2^*, \dots, b_n^*\right]$ the corresponding Gram–Schmidt orthogonal basis (B^* spans the same linear subspace as B, but not necessarily generates the same lattice). Then the shortest vector in B^* gives a lower bound on the required value of ε.

Lemma 1. *Let $\Lambda = \Lambda(B)$ be a lattice. Then*

$$\inf\left\{\|z\|_2 : z \in \Lambda \setminus \{0\}\right\} \geqslant \min_i \|b_i^*\|_2.$$

Proof. Any vector z in the span of B may be expressed as a linear combination of vectors in B^*:

$$z = \sum_{i=1}^{n} \tfrac{\langle z, b_i^* \rangle}{\langle b_i^*, b_i^* \rangle} b_i^*.$$

Furthermore, since B^* is an orthogonal basis, we have

$$\|z\|^2 = \sum_{i=1}^{n} \left\| \tfrac{\langle z, b_i^* \rangle}{\langle b_i^*, b_i^* \rangle} b_i^* \right\|^2 = \sum_{i=1}^{n} \tfrac{\langle z, b_i^* \rangle^2}{\langle b_i^*, b_i^* \rangle^2} \|b_i^*\|^2.$$

Suppose that $z \in \Lambda \setminus \{0\}$, i.e., $z = \sum_{i=1}^{n} x_i b_i$ for some integers $x_1, x_2, \ldots, x_n$, not all equal to 0, and let k be the biggest index such that $x_k \neq 0$. Then

$$\|z\|^2 = \sum_{i=1}^{n} \frac{\langle z, b_i^* \rangle^2}{\langle b_i^*, b_i^* \rangle^2} \|b_i\|^2 \geqslant \frac{\langle z, b_k^* \rangle^2}{\langle b_k^*, b_k^* \rangle^2} \|b_k\|^2 = \frac{\langle z, b_k^* \rangle^2}{\langle b_k^*, b_k^* \rangle}.$$

Now, it suffices to show that $|\langle z, b_k^* \rangle| \geqslant \langle b_k^*, b_k^* \rangle$; this will imply that $\|z\| \geqslant \|b_k^*\|$, and consequently, $\|z\| \geqslant \min_i \|b_i^*\|$ for all $z \in \Lambda \setminus \{0\}$. By the choice of k, $x_i = 0$ for all $i > k$. Since b_k^* is orthogonal to the span of vectors $b_1^*, b_2^*, \ldots, b_{k-1}^*$, which is also the span of vectors $b_1, b_2, \ldots, b_{k-1}$, we have $\langle b_i, b_k^* \rangle = 0$ for all $i < k$. Finally, $\langle b_k, b_k^* \rangle = \langle b_k^*, b_k^* \rangle$ follows immediately from the description of the Gram–Schmidt orthogonalization procedure. All together, this yields

$$|\langle z, b_k^* \rangle| = \left| \sum_{i=1}^{k} x_i \cdot \langle b_i, b_k^* \rangle \right| = |x_i| \cdot |\langle b_k, b_k^* \rangle| = |x_i| \cdot \langle b_k^*, b_k^* \rangle \geqslant \langle b_k^*, b_k^* \rangle,$$

because $|x_k| \geqslant 1$. This completes the proof. □

Thus, lattices are indeed discrete subgroups of $\mathbb{R}^n$. Moreover, we obtained a reasonable lower bound on the norm of the shortest vector in a lattice. However, this bound depends on the choice of a basis B, and even on the order of vectors in B.

1.2 Discrete subgroups of $\mathbb{R}^n$ are lattices

It remains to show that every discrete subgroup of $\mathbb{R}^n$ is a lattice. Let Λ be a discrete subgroup of $\mathbb{R}^n$. We need to show that there is a set of linearly independent vectors $B = \left[b_1, b_2, \ldots, b_k\right]$ such that $\Lambda = \Lambda(B)$. First, we show that there is a lattice vector attaining the infimum in Lemma 1.

Lemma 2. *Let $\Lambda \subseteq \mathbb{R}^n$ be a discrete group. Then there is a vector $b_1 \in \Lambda$ such that*

$$\|b_1\| = \lambda_1 := \inf\left\{\|z\| : z \in \Lambda \setminus \{0\}\right\}.$$

Proof. Let $z_1, z_2, \ldots$ be a sequence of vectors from Λ such that the sequence of their norms $\|z_i\|$ converges to λ_1. We may assume that all z_i's belong to the closed ball $\left\{x : \|x\| \leqslant 2\lambda_1\right\}$, which is a compact set. Then there is a subsequence $z_{i_1}, z_{i_2}, \ldots$ that converges to some vector, say z. Furthermore, there is an index j_0 such that $\|z_{i_j} - z\| \leqslant \frac{\varepsilon}{2}$ for all $j > j_0$ (where ε comes from the definition of a discrete group). Thus, for any $j, k > j_0$, we have

$$\|z_{i_j} - z_{i_k}\| \leqslant \|z_{i_j} - z\| + \|z - z_{i_k}\| \leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

and since both z_{i_j} and z_{i_k} belong to Λ, we must have $z_{i_j} = z_{i_k}$. Consequently, $z = z_{i_j}$ is also a vector from Λ, and we may assign $b_1 = z$. □

It is easy to see that every vector $z \in \Lambda$, belonging to the span of b_1, is an integer multiple of b_1. Indeed, if $\alpha b_1 \in \Lambda$ and α is not an integer, then the vector $b_1' = (\alpha - \lfloor \alpha \rfloor) b_1$ also belongs to Λ but $\|b_1'\| < \|b_1\|$, a contradiction.

Now, we proceed by induction, assuming that $\|\cdot\|$ is the ℓ_2-norm. Suppose that we have constructed vectors $b_1, b_2, \ldots, b_k$ such that every vector $z \in \Lambda$ in the span of $b_1, b_2, \ldots, b_k$, is an integral linear combination of these vectors. Let L denote the span of $b_1, b_2, \dots, b_k$. If $\Lambda \subseteq L$, there is nothing to do. Otherwise, we define b_{k+1} as a vector from $\Lambda \setminus L$, whose distance to L is as small as possible. Existence of such a vector can be shown in a similar way to the proof of Lemma 2. Indeed, let δ denotes the infimum of the distances $d(z, L)$ from $z \in \Lambda \setminus L$ to L. Every vector $z \in \Lambda \setminus L$ can be expressed as $z = x + z^*$, where $x \in L$ and $z^* \in L^\perp$. Then $d(z, L) = \|z^*\|$. Particularly, if $z = x + z^*$ and $x = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_k b_k$, then the vector

$$z^* + \sum_{i=1}^{k} (\alpha_i - \lfloor \alpha_i \rfloor) b_i$$

is at the same distance $\|z^*\|$ from L as vector z. Therefore, we may restrict our attention onto vectors $z = x + z^*$, where $0 \leqslant \alpha_i \leqslant 1$ for all i (i.e., x is taken from the closed parallelepiped). Let $z_1, z_2, \ldots$ be a sequence of vectors from $\Lambda \setminus L$, satisfying the above assumption, such that the sequence $\|z_i^*\|$ converges to δ. We may further assume that $\|z_i^*\| \leqslant 2\delta$ for all i. Then all z_i's are taken from a compact set, and therefore, there is a convergent subsequence $z_{i_1}, z_{i_2}, \ldots$. As above, we may argue that starting from some index j_0, all vectors z_{i_j} are the same, say $z_{i_j} = z$. Then $\|z^*\| = \delta > 0$ and we assign $b_{k+1} = z$.

It remains to show that all vectors from Λ belonging to the span of $L \cap \{b_{k+1}\}$ can be expressed as an integral linear combination of vectors $b_1, b_2, \ldots, b_{k+1}$. Indeed, suppose that $z = \sum_{i=1}^{k+1} \alpha_i b_i$ is a vector from Λ. If α_{k+1} is not an integer, then the vector

$$z' = \sum_{i=1}^{k} \alpha_i b_i + (\alpha_{k+1} - \lfloor \alpha_{k+1} \rfloor) b_{k+1}$$

is closer to L than b_{k+1}:

$$d(z', L) = (\alpha_{k+1} - \lfloor \alpha_{k+1} \rfloor) \|b_{k+1}^*\| < \|b_{k+1}^*\| = d(b_{k+1}, L),$$

a contradiction to our choice of b_{k+1}. Therefore, α_{k+1} is an integer. Then the vector $z - \alpha_{k+1} b_{k+1}$ belongs to $\Lambda \cap L$, and hence, can be expressed as an integral linear combination of vectors $b_1, b_2, \ldots, b_k$.

After at most n steps, the process terminates. Thus, we proved the following theorem.

Theorem 3. *A set $\Lambda \subseteq \mathbb{R}^n$ is a lattice if and only if it is a discrete group.*

2 Fundamental parallelepiped

Let $\Lambda = \Lambda(B)$ be a full-dimensional lattice in $\mathbb{R}^n$. The set

$$\Pi(B) := \left\{ Bx : x \in [0,1)^n \right\}$$

is called the *fundamental parallelepiped* associated to B. The volume of the fundamental parallelepiped $\mathrm{vol}(B)$ is exactly the absolute value of the determinant of B, $|\det(B)|$, which, as we know from the previous lectures, is the same for all bases of lattice Λ. This suggests the way to generalize the notion of the lattice determinant to lower-dimensional lattices, too.

Let $B \in \mathbb{R}^{n\times k}$ be a matrix of full column rank and let $\Lambda = \Lambda(B)$ be the lattice generated by B. We define the *determinant* of Λ as

$$\det(\Lambda) := \mathrm{vol}(\Pi(B)) = \sqrt{\det(B^{\mathrm{T}}B)},$$

where by $\mathrm{vol}(\Pi(B))$ we mean the relative volume of $\Pi(B)$, i.e., its volume in the linear space spanned by B. It is straight-forward to show that this quantity is invariant over unimodular transformations of B, and therefore, $\det(\Lambda)$ is well-defined.

We shall need the following property of fundamental parallelepipeds.

Lemma 4. *Let $\Lambda = \Lambda(B)$ be a full-dimensional lattice in $\mathbb{R}^n$. Then the sets*

$$z + \Pi(B) := \{z + x : x \in \Pi(B)\}, \qquad z \in \Lambda,$$

form a partition of $\mathbb{R}^n$.

Proof. We show that every vector $x \in \mathbb{R}^n$ can be uniquely expressed as $x = z + y$, where $z \in \Lambda$ and $y \in \Pi(B)$. Since B spans $\mathbb{R}^n$, we have

$$x = \sum_{i=1}^{n} \alpha_i b_i = \sum_{i=1}^{n} \lfloor \alpha_i \rfloor b_i + \sum_{i=1}^{n} \{\alpha_i\} b_i$$

for some numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$; here $\lfloor \alpha \rfloor$ denotes the largest integer not exceeding α and let $\{\alpha\}$ denotes $\alpha - \lfloor \alpha \rfloor$. Now, the vector $z = \sum_{i=1}^{n} \lfloor \alpha_i \rfloor b_i$ belongs to the lattice Λ, while $y = \sum_{i=1}^{n} \{\alpha_i\} b_i$ belongs to the fundamental parallelepiped $\Pi(B)$, and the claim follows.

Suppose that $x = z + y = z' + y'$ with $z, z' \in \Lambda$ and $y, y' \in \Pi(B)$. Then the vector $z - z'$ also belongs to the lattice, and therefore, can be expressed as

$$z - z' = \sum_{i=1}^{n} \lambda_i b_i, \qquad \lambda_i \in \mathbb{Z},\ i = 1, 2, \ldots, n.$$

On the other hand,

$$z - z' = y' - y = \sum_{i=1}^{n} \mu_i b_i, \qquad -1 < \mu_i < 1,\ i = 1, 2, \ldots, n,$$

since both y and y' belong to the fundamental parallelepiped $\Pi(B)$. The vectors $b_1, b_2, \ldots, b_n$ are linearly independent, and therefore, both expressions must be the same, i.e., $\lambda_i = \mu_i$ for each i. But then the only possible choice is $\lambda_i = 0$ for each i, which means $z = z'$ and $y = y'$. □

3 Minkowski's theorem

In this section, we consider the classical result of Minkowski, which, in some sense, originated the whole geometry of numbers. Intuitively, it established the connexion between the "geometric" properties of the sets (convexity, symmetry, volume) and its arithmetic properties (existence of an integral vector in a set).

As it is quite common nowadays, we shall not follow the original proof of Minkowski, but exploit a later result of Blichfeldt.

Theorem 5 (Blichfeldt)**.** *Let Λ be a full-dimensional lattice in $\mathbb{R}^n$ and let $C \subseteq \mathbb{R}^n$ be a measurable set. Suppose that either*

(a) $\mathrm{vol}(C) > m \cdot \det(\Lambda)$*, or*

(b) $\mathrm{vol}(C) \geqslant m \cdot \det(\Lambda)$ *and C is compact.*

Then there are $m+1$ vectors $x_0, x_1, \dots, x_m \in C$ such that $x_i - x_j \in \Lambda$ for each i, j.

Proof. For simplicity, we give a proof for the case $m = 1$. Let B be a basis of Λ and suppose that $\mathrm{vol}(C) > \det(\Lambda)$. We consider the sets

$$C_z := C \cap (z + \Pi(B)), \qquad z \in \Lambda.$$

By Lemma 4, these sets partition C, and therefore,

$$\mathrm{vol}(C) = \sum_{z \in \Lambda} \mathrm{vol}(C_z).$$

Now, consider the translates $C_z - z = \{x - z : x \in C_z\}$. Clearly, $C_z - z = (C - z) \cap \Pi(B) \subseteq \Pi(B)$. Now, we argue that these translates $C_z - z$ cannot be pairwise disjoint. Indeed, since $\mathrm{vol}(C_z - z) = \mathrm{vol}(C_z)$, the total volume of all these sets is

$$\sum_{z \in \Lambda} \mathrm{vol}(C_z - z) = \sum_{z \in \Lambda} \mathrm{vol}(C_z) = \mathrm{vol}(C) > \det(\Lambda) = \mathrm{vol}(\Pi(B)).$$

As all the sets $C_z - z$ lie in $\Pi(B)$, there must be $z_0, z_1 \in \Lambda$ such that $(C_{z_0} - z_0) \cap (C_{z_1} - z_1)$ is non-empty. Let y be a vector in $(C_{z_0} - z_0) \cap (C_{z_1} - z_1)$. If we define $x_0 = y + z_0 \in C_{z_0} \subseteq C$ and $x_1 = y + z_1 \in C_{z_1} \subseteq C$, then $x_1 - x_0 = z_1 - z_0 \in \Lambda$. This completes the proof of Part (a). Part (b) follows by a compactness argument, similarly to what we did in the proof of Theorem 3. Considering the sets $(1+\varepsilon)C$ with $\varepsilon \to 0$, we find a sequence of vector pairs (x_0, x_1) such that $x_1 - x_0 \in \Lambda$. Since C is a compact set, there is a subsequence of this sequence that converges to some pair of vectors in C. Then the sequence of the differences $x_1 - x_0$ also converges, and since all these vectors belong to Λ, the limit also belongs to Λ.

The proof for $m > 1$ is very similar, except that we use inequality $\mathrm{vol}(C) > m \cdot \mathrm{vol}(\Pi(B))$ to argue that there is a vector y contained in $m+1$ of the sets $C_z - z$. □

Theorem 6. *Let Λ be a full-dimensional lattice in $\mathbb{R}^n$ and let $C \subseteq \mathbb{R}^n$ be a convex set symmetric about the origin (i.e., $x \in C$ implies $-x \in C$). Suppose that either*

(a) $\mathrm{vol}(C) > m \cdot 2^n \cdot \det(\Lambda)$*, or*

(b) $\mathrm{vol}(C) \geqslant m \cdot 2^n \cdot \det(\Lambda)$ *and C is compact.*

Then there are m different pairs of vectors $\pm z_1, \pm z_2, \dots, \pm z_m \in C \cap \Lambda \setminus \{0\}$.

Proof. It is easy to see that the volume of the set $\frac{1}{2}C = \{\frac{1}{2}x : x \in C\}$ is $2^{-n}\mathrm{vol}(C)$, and therefore, we can apply Theorem 5 to find vectors $\frac{1}{2}x_0, \frac{1}{2}x_1, \dots, \frac{1}{2}x_m \in \frac{1}{2}C$ such that $\frac{1}{2}x_i - \frac{1}{2}x_j \in \Lambda$ for all i and j. Without loss of generality, we assume that vector x_0 is lexicographically smaller than any other vector $x_1, x_2, \dots, x_m$ (we write $x_0 \prec x_i$ for all $i > 0$). Define

$$z_i = \tfrac{1}{2}x_i - \tfrac{1}{2}x_0, \qquad i = 1, 2, \dots, m.$$

Clearly, all z_i's are different; moreover, since $0 \prec z_i$ for all i, we have $z_i \neq -z_j$ for all i and j. It remains to show that $z_i \in C$. Indeed, $x_0 \in C$ implies $-x_0 \in C$, as C is symmetric about the origin, and $\frac{1}{2}x_i - \frac{1}{2}x_0 = \frac{1}{2}x_i + \frac{1}{2}(-x_0) \in C$, as C is convex. □

4 Applications of Minkowski's theorem

Now, we consider some applications of Minkowski's theorem. We shall not use them on our course, the only purpose of these applications is to demonstrate how wide is the range of these applications.

4.1 Dirichlet's theorem on Diophantine approximation

Let α be a real number and suppose that we wish to approximate α with rational numbers. Clearly, we can do it with any precision, but we put an extra requirement on the denominator of a rational number: it should not exceed a given Q. Obviously, we can find a rational number p/Q such that $\left|\alpha - \frac{p}{Q}\right| \leqslant \frac{1}{Q}$. But, in fact, we can do much better. The following theorem was derived by Dirichlet using rather elementary methods. However, it can also be viewed as a direct corollary of Minkowski's theorem.

Theorem 7 (Dirichlet)**.** *Let α be a real number and Q a positive integer. Then there are integers p and q with* $0 < q \leqslant Q$ *and*

$$\left|\alpha - \tfrac{p}{Q}\right| \leqslant \tfrac{1}{qQ}.$$

Proof. We assume that $Q > 1$. Consider the following set of points C in $\mathbb{R}^d$ defined by the following inequalities:

$$y \leqslant \alpha x + \tfrac{1}{Q}, \qquad y \geqslant \alpha x - \tfrac{1}{Q}, \qquad x \leqslant Q, \qquad x \geqslant -Q.$$

Thus, C is a closed parallelepiped of volume $\mathrm{vol}(C) = 4Q\frac{1}{Q} = 4$, symmetric about the origin. By Minkowski's theorem, it contains a point $(q, p) \in \mathbb{Z}^2$ (the determinant of lattice $\mathbb{Z}^2$ is 1). We may assume that $q \geqslant 0$. Moreover, $q = 0$ is impossible, since then we would have $-\frac{1}{Q} \leqslant p \leqslant \frac{1}{Q}$, whence $p = 0$. Therefore, $0 < q \leqslant Q$ holds. Yet, the first two inequalities imply

$$|p - \alpha q| \leqslant \tfrac{1}{Q}. \qquad \square$$

We remark that the theorem can be generalized to the case of *simultaneous Diophantine approximation*, where we are given n real numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ and a positive integer Q, and the task is to find rational numbers $\frac{p_1}{q}, \frac{p_2}{q}, \ldots, \frac{p_n}{q}$ with $0 < q \leqslant Q$, approximating $\alpha_1, \alpha_2, \ldots, \alpha_n$, respectively.

4.2 Lagrange's four-square theorem

The following theorem was first proved by Lagrange and states that every positive integer can be expressed as the sum of four squares of integers. It is also a consequence of Minkowski' theorem, although not as straight-forward as our previous example.

Theorem 8. *For every positive integer x, there are integers x_1, x_2, x_3, and x_4 such that*

$$x = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Proof. First, we remark that we only need to consider integers x that are prime: if

$$x = x_1^2 + x_2^2 + x_3^2 + x_4^2 \qquad \text{and} \qquad y = y_1^2 + y_2^2 + y_3^2 + y_4^2,$$

then

$$\begin{aligned} xy = &(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+ (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 \\ &+ (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2. \end{aligned}$$

Thus, let x be a prime number. First, we show that there are integers y and z such that $y^2 + z^2 + 1 \equiv 0 \pmod{x}$. For $x = 2$ this is trivially true; otherwise, x is odd. Consider the set

$$S_1 := \left\{y^2 \bmod x : 0 \leqslant y \leqslant \tfrac{x-1}{2}\right\}.$$

It is easy to see that $(y_1 \bmod x) \neq (y_2 \bmod x)$ for different $0 \leqslant y_1, y_2 \leqslant \frac{x-1}{2}$: otherwise

$$(y_1 - y_2)(y_1 + y_2) = (y_1^2 - y_2^2) \equiv 0 \pmod{x},$$

but both terms in the product $(y_1 - y_2)(y_1 + y_2)$ are not divisible by x, a contradiction. Consequently, $|S_1| = \frac{x+1}{2}$. Similarly, we may show that

$$S_2 := \left\{-z^2 - 1 \bmod x : 0 \leqslant z \leqslant \tfrac{x-1}{2}\right\}.$$

has cardinality $\frac{x+1}{2}$. Therefore, these two sets must intersect, and this intersection yields y and z as required.

Now, we choose a suitable lattice and a suitable set to apply Minkowski's theorem. We define $\Lambda = \Lambda(B)$, where

$$B = \begin{bmatrix} x & 0 & y & z \\ 0 & x & z & -y \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

For every vector $\left[x_1, x_2, x_3, x_4\right] = B\left[\lambda_1, \lambda_2, \lambda_3, \lambda_4\right]^{\mathrm{T}} \in \Lambda$, we have

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= (x\lambda_1 + y\lambda_3 + z\lambda_4)^2 + (x\lambda_2 + z\lambda_3 - y\lambda_4)^2 + \lambda_3^2 + \lambda_4^2 \\ &\equiv (1 + y^2 + z^2)(\lambda_3^2 + \lambda_4^2) \pmod{x} \\ &\equiv 0 \pmod{x}. \end{aligned}$$

Yet, we have $\det(\Lambda) = x^2$. Consider the ball

$$\mathscr{B} = \left\{\left[x_1, x_2, x_3, x_4\right] : x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2x\right\}.$$

The volume of this ball is

$$\operatorname{vol}(\mathscr{B}) = \frac{1}{2}\pi^2(\sqrt{2x})^4 = 2\pi^2 x^2 > 2^4 x^2.$$

Therefore, by Minkowski's theorem, there is a non-zero vector $\left[x_1, x_2, x_3, x_4\right] \in \Lambda \cap \mathscr{B}$, i.e.,

$$0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2x \qquad \text{and} \qquad x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod x,$$

and the latter is only possible when $x = x_1^2 + x_2^2 + x_3^2 + x_4^2$. □