UGC SUMMER SCHOOL
MINICOURSE ON GEOMETRY OF NUMBERS

MARTA PIEROPAN

Contents

The Geometry of Numbers is an important branch of number theory initiated by Hermann Minkowski at the end of the 19th century. This minicourse is based on [OLD00], [CF67], [FT93, §IV.2]

We consider the vector space $\mathbb{R}^n$ with a fixed basis $e_1, \dots, e_n$. We write $\underline{x}$ for a vector in $\mathbb{R}^n$ and $(x_1, \dots, x_n)$ for its coordinates with respect to the fixed basis, so that $\underline{x} = \sum_{i=1}^n x_i e_i$. We write $\underline{0}$ for the origin of $\mathbb{R}^n$, i.e., the vector with all coordinates equal to 0. The induced Euclidean norm is $\|\underline{x}\| = \sqrt{x_1^2 + \cdots + x_n^2}$. The induced Lebesgue measure satisfies $\mathrm{vol}([0,1]^n) = \int_{0 \le x_i \le 1, 1 \le i \le n} dx_1 \cdots dx_n = 1$.

1. Lattices

The *standard lattice* in $\mathbb{R}^n$ is the set of vectors with integer coordinates

$$\Lambda_s = \{\underline{x} \in \mathbb{R}^n : x_1, \dots, x_n \in \mathbb{Z}\} \subseteq \mathbb{R}^n.$$

For us a *lattice* Λ in $\mathbb{R}^n$ is the image of a group homomorphism $\mathbb{Z}^n \to \mathbb{R}^n$ such that Λ spans $\mathbb{R}^n$.

Remark 1.1. For every lattice $\Lambda \subseteq \mathbb{R}^n$ there is a unique linear transformation $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ such that $\Lambda = \varphi(\Lambda_s)$.

Exercise 1.2. Show that the linear map φ in Remark 1.1 is an isomorphism.

Date: August 18, 2023.

The *fundamental parallelepiped* of the lattice Λ is

$$F(\Lambda) = \sum_{i=1}^{n} [0,1)\varphi(e_i).$$

The *determinant* of the lattice Λ is

$$\det(\Lambda) = \left|\det(\varphi(e_i))_{1\leq i\leq n}\right|,$$

i.e., the determinant of the matrix whose columns are the coordinates of the vectors $\varphi(e_1), \ldots, \varphi(e_n)$.

Exercise 1.3. Show that a subset $\Lambda \subseteq \mathbb{R}^n$ is a lattice if and only if Λ is a subgroup of $\mathbb{R}^n$ that spans $\mathbb{R}^n$ and there is a real number $\varepsilon > 0$ such that

$$\Lambda \cap \{\underline{x} \in \mathbb{R}^n : \|\underline{x}\| \leq \varepsilon\} = \{\underline{0}\}.$$

2. Guiding questions of geometry of numbers

Given a lattice Λ in $\mathbb{R}^n$ we can ask the following questions.

Question 1: which subsets of $\mathbb{R}^n$ contain points of Λ?
Question 2: how many points of Λ lie in a given subset of $\mathbb{R}^n$?

These are the guiding questions of geometry of numbers. We will start by addressing the first one as follows.

Exercise 2.1. Show that every closed disk of radius at least 1 in $\mathbb{R}^2$ contains at least on point of Λ_s.

Exercise 2.2. Show that every square of sidelength at least 2 in $\mathbb{R}^2$ contains at least a point of Λ_s.

The exercises here above show that sufficiently large disks and squares always contain lattice points, however small disks and squares don't need to contain any lattice points. Find some examples.

Are the bounds in the exercises here above sharp?

Up to translation we can always assume that our set contains a lattice point, for example $\underline{0}$. Hence, it makes sense to ask whether a subset of $\mathbb{R}^n$ containing $\underline{0}$ contains any other point of Λ.

It is easy to show that every square S in $\mathbb{R}^2$ centered at $\underline{0}$ and with sidelength smaller than 2 satisfies $S \cap \Lambda_s = \{\underline{0}\}$. Similarly, every disk D in $\mathbb{R}^2$ centered at $\underline{0}$ and with radius smaller than 1 satisfies $D \cap \Lambda_s = \{\underline{0}\}$.

From these examples, we see that the answer to Question 1 depends on the size of the subsets.

3. Minkowski's Fundamental Theorem

A set $S \subseteq \mathbb{R}^n$ is said to be

- *bounded* if there exists a real number $B > 0$ such that $\|\underline{x}\| \leq B$ for all $\underline{x} \in S$;
- *convex* if for all $\underline{x}$ and $\underline{y}$ in S the segment between $\underline{x}$ and $\underline{y}$ is wholly contained in S;
- *centrally symmetric* if $-\underline{x} \in S$ for all $\underline{x} \in S$.

Here, the segment between two vectors $\underline{x}$ and $\underline{y}$ in $\mathbb{R}^n$ is the set

$$\{\lambda\underline{x} + (1-\lambda)\underline{y} : 0 \leq \lambda \leq 1\}.$$

For a bounded convex set $S \subseteq \mathbb{R}^n$, the indicator function

$$\mathbf{1}_S : \mathbb{R}^n \to \mathbb{R}^n, \quad \underline{x} \mapsto \begin{cases} 1 & \text{if } \underline{x} \in S, \\ 0 & \text{if } \underline{x} \notin S, \end{cases}$$

is Riemann integrable [FT93, Exercise IV.10]. We define the volume of S as $\mathrm{vol}(S) = \int_{\mathbb{R}^n} \mathbf{1}_S$.

Exercise 3.1. Show that if $S \subseteq \mathbb{R}^n$ is convex and centrally symmetric, then $\underline{0} \in S$.

Exercise 3.2. Let $S \subseteq \mathbb{R}^n$ be a convex set that contains three non-collinear points A, B, C. Show that S contains the triangle with vertices A, B, C.

Exercise 3.3. Show that a closed set $S \subseteq \mathbb{R}^2$ with nonempty interior is convex if and only if for every point P on the boundary of S there exists a line L through P such that the whole of S lies on one side of L. Here, the boundary of S is the difference between the closure and the interior of S.

Exercise 3.4. Show that the intersection of two convex sets is convex.

Theorem 3.5 (Minkowski's Fundamental Theorem, 1889)**.** *Let $S \subseteq \mathbb{R}^n$ be a bounded, convex set that is centrally symmetric and such that $\mathrm{vol}(S) > 2^n$. Then there exists a point $\underline{x} \in S \cap \Lambda_s$ such that $\underline{x} \neq \underline{0}$.*

Remark 3.6. For an arbitrary lattice $\Lambda \subseteq \mathbb{R}^n$, the same conclusion holds provided we replace the assumption $\mathrm{vol}(S) > 2^n$ by $\mathrm{vol}(S) > 2^n \det(\Lambda)$.

Exercise 3.7. Show that the assumptions on the convexity of S and on the volume are necessary.

Proof of Theorem 3.5. Let $Q = [-1,1]^n$ be the cube of volume 2^n centered at $\underline{0}$. Then $\mathbb{R}^n = \bigcup_{\underline{u} \in 2\Lambda_s} (Q + \underline{u})$ is the union of translates of Q by vectors with even integer coordinates. Since S is bounded,

there is a finite subset $U \subseteq 2\Lambda_s$ such that $S \subseteq \bigcup_{\underline{u}\in U}(Q + \underline{u})$. For every $\underline{u} \in U$, let $S_{\underline{u}} = ((Q + \underline{u}) \cap S) - \underline{u}$. Then $S_{\underline{u}} \subseteq Q$ for every $\underline{u} \in U$. Since $\mathrm{vol}(S) > 2^n$ and $\mathrm{vol}(Q) = 2^n$, there must be distinct points $\underline{u}, \underline{v} \in U$ such that $S_{\underline{u}}$ and $S_{\underline{v}}$ overlap. Let $\underline{x} \in S_{\underline{u}} \cap S_{\underline{v}}$. Then there are distinct points $\underline{y}, \underline{z} \in S$ such that $\underline{x} = \underline{y} - \underline{u} = \underline{z} - \underline{v}$. Since S in centrally symmetric, we have $-\underline{z} \in S$. Since S is convex $(\underline{y} - \underline{z})/2 \in S$. Since $(\underline{y} - \underline{z})/2 = (\underline{u} - \underline{v})/2$ and $\underline{u}, \underline{v} \in 2\Lambda_s$, we conclude that $(\underline{y} - \underline{z})/2 \in \Lambda_s \cap S$. Finally, $(\underline{y} - \underline{z})/2 \neq \underline{0}$, as $\underline{y}$ and $\underline{z}$ are distinct. □

Exercise 3.8. Deduce Remark 3.6 from Theorem 3.5 and a suitable linear transformation.

Remark 3.9. If in addition S is a closed subset, the conclusion of Theorem 3.5 holds also if $\mathrm{vol}(S) = 2^n$. Indeed, since S is closed, the smallest distance of any point of $\Lambda_s \setminus S$ from S is a positive real number δ. Hence, we can enlarge S by $\delta/2$ in every direction, to obtain a bounded, convex, centrally symmetric set S' with volume $\mathrm{vol}(S') > \mathrm{vol}(S)$ and $S' \cap \Lambda_s = S \cap \Lambda_s$.

The proof presented here is based on Blichfeldt's approach in [OLD00, Problem 5.3.3]. Minkowski's original proof can be found in [OLD00, §5.3]. Additional reading: Blichfeldt's theorems in [OLD00, §9] or in [FT93, §IV.2].

4. Applications of Minkowski's Fundamental Theorem

Exercise 4.1 (Simultaneous Diophantine Approximation [OLD00, §6.6])**.**

Let $\alpha_1, \ldots, \alpha_n$ be irrational real numbers. Show that there exist infinitely many sets of integers $p_1, \ldots, p_n, p$ with $p \geq 1$ such that

$$\left| \frac{p_i}{p} - \alpha_i \right| \leq \frac{1}{p^{1+\frac{1}{n}}}$$

for all $i \in \{1, \ldots, n\}$, by applying Minkowski's Fundamental Theorem to

$$S_\epsilon = \{\underline{x} \in \mathbb{R}^{n+1} : |x_i - \alpha_i x_{n+1}| \leq \epsilon \ \forall i \in \{1, \ldots, n\}, |x_{n+1}| \leq \epsilon^{-n}\}$$

for any $\epsilon \in (0, 1)$.

Exercise 4.2. (Lagrange's Four Squares Theorem [OLD00, §8.6])
An integer x is said to be a sum of four squares if there are $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ such that $x = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Step 1: Show that if two integers x and y are both sums of four squares then the product xy is a sum of four squares.

Step 2: Show that if x is a prime number then there are $y, z \in \mathbb{Z}$ such that $x \mid y^2 + z^2 + 1$. If $x > 2$ consider the sets

$$S_1 = \{y^2 \mod x : 0 \leq y \leq (x-1)/2\},$$
$$S_2 = \{-z^2 - 1 \mod x : 0 \leq z \leq (x-1)/2\},$$

and show that $S_1 \cap S_2 \neq \emptyset$ by computing their cardinalities.

Let $\varphi : \mathbb{R}^4 \to \mathbb{R}^4$ given by the matrix

$$\begin{pmatrix} x & 0 & y & z \\ 0 & x & z & -y \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let $\Lambda = \varphi(\Lambda_s)$. Let

$$S = \{\underline{x} \in \mathbb{R}^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2x\}.$$

Step 3: Show that $x \mid x_1^2 + x_2^2 + x_3^2 + x_4^2$ for all $\underline{x} \in \Lambda$.

Step 4: Apply Minkowski's Fundamental Theorem to S for the lattice Λ.

Step 5: Combine Steps $1 - 4$ to show that every positive integer x is a sum of four squares.

5. Number of lattice points in squares and disks

In this section we address Question 2 in two specific examples.

5.1. **Squares.** Let $S(L) = [-L, L]^2$ be the square in $\mathbb{R}^2$ centered at $\underline{0}$ and with sidelength $2L$. Let $N(S(L))$ be the cardinality of $S(L) \cap \Lambda_s$. We want to estimate the size of $N(S(L))$. One approach consists in drawing for each point $P \in S(L) \cap \Lambda_s$ the fundamental parallelepiped with vertex P, that is, $F(\Lambda_s) + P$. Since the area of $F(\Lambda_s)$ is 1, the number $N(S(L))$ is equal to the area of the region $\cup_{P \in S(L) \cap \Lambda_s} (F(\Lambda_s) + P)$. We observe that this region is contained in the square $S(L+1)$ and contains the square $S(L-1)$. Hence, its area is bounded above by $\mathrm{vol}(S(L+1))$ and below by $\mathrm{vol}(S(L-1))$. Thus

$$\mathrm{vol}(S(L-1)) \leq N(S(L)) \leq \mathrm{vol}(S(L+1))$$
$$(2(L-1))^2 \leq N(S(L)) \leq (2(L+1))^2$$
$$2L^2 - 8L + 4 \leq N(S(L)) \leq 4L^2 + 8L + 4.$$

Dividing both sides by $4L^2$ and taking the limit we observe that

$$\lim_{L \to \infty} \frac{N(S(L))}{4L^2} = 1.$$

Thus $N(S(L))$, as a function of L, grows asymptotically like $4L^2$. Since

$$4L^2 - 8L - 4 \leq 4L^2 - 8L + 4 \leq N(S(L)) \leq 4L^2 + 8L + 4,$$

we can estimate the difference as follows

$$|N(S(L)) - 4L^2| \leq 8L + 4.$$

Notation 5.1. Given two functions $f, g : \mathbb{R}_{>0} \to \mathbb{R}$ we write

$$f = O(g)$$

if there is a real number $C > 0$ such that $|f(x)| \leq Cg(x)$ for all $x \in \mathbb{R}_{>0}$.

With the notation just introduced, we have

$$N(S(L)) = 4L^2 + O(L).$$

5.2. **Disks.** Let $D(r)$ be the disk in $\mathbb{R}^2$ centered at the origin and with radius r. Let $N(D(r))$ be the cardinality of $D(r) \cap \Lambda_s$. We want to estimate the size of $N(D(r))$. As in the previous example, we can draw a fundamental parallelepiped with vertes P for every $P \in D(r) \cap \Lambda_s$. The union of such parallelepipeds is contained in the disk $D(r + \sqrt{2})$ and contains the disk $D(r - \sqrt{2})$. Thus

$$\text{vol}(D(r - \sqrt{2})) \leq N(D(r)) \leq \text{vol}(D(r + \sqrt{2}))$$
$$\pi(r - \sqrt{2})^2 \leq N(D(r)) \leq \pi(r + \sqrt{2})^2,$$

and as in the previous example, we conclude that

$$\lim_{r\to\infty} \frac{N(D(r))}{\pi r^2} = 1$$

and

$$N(D(r)) = \pi r^2 + O(r).$$

An analogous argument is presented in [OLD00, §4.1].

5.3. **Two equivalent norms.** The disk

$$D(r) = \{(x, y) \in \mathbb{R}^2 : \sqrt{x^2 + y^2} \leq r\}$$

is a closed ball for the Euclidean topology, i.e., the topology induced by the Euclidean norm $\|(x, y)\| = \sqrt{x^2 + y^2}$.

The square

$$S(L) = \{(x, y) \in \mathbb{R}^2 : |x|, |y| \leq L\}$$

is a closed ball for the topology induced by the sup norm $\|(x, y)\|_\infty = \max\{|x|, |y|\}$.

These two norms are equivalent, in the sense that $\|\cdot\|_\infty = O(\|\cdot\|)$ and $\|\cdot\| = O(\|\cdot\|_\infty)$, as you can show with the following exercise.

Exercise 5.2. Show that for all $(x, y) \in \mathbb{R}^2$ the following inequalities holds:

$$\max\{|x|, |y|\} \leq \sqrt{x^2 + y^2},$$
$$\sqrt{x^2 + y^2} \leq \sqrt{2}\max\{|x|, |y|\}.$$

6. Number of lattice points in more general shapes

Minkowski's Fundamental Theorem shows the existence of lattice points in convex centrally symmetric sets of sufficiently large volume. How many lattice points are there in these sets? The examples of the squares and disks suggest that the number of points has a precise dependence on the volume of the region. This is in fact true also for convex centrally symmetric sets and more general sets.

Exercise 6.1. Let $S \subseteq \mathbb{R}^n$ be a bounded, convex, centrally symmetric set. Show that

$$LS = \{\underline{x} \in \mathbb{R}^n : \frac{1}{L}\underline{x} \in S\}$$

is bounded, convex and centrally symmetric for all $L > 0$.

Recall that the indicator function $\mathbf{1}_S$ of a bounded convex set is Riemann integrable.

Theorem 6.2. *Let $S \subseteq \mathbb{R}^n$ be a bounded set such that $\mathbf{1}_S$ is Riemann integrable. Let $N(LS)$ be the cardinality of $LS \cap \Lambda_s$. Then*

$$\lim_{L\to\infty} \frac{N(LS)}{L^n} = \mathrm{vol}(S).$$

Proof. Since S is bounded there is $B > 0$ such that $S \subseteq [-B, B]^n$. Then

$$\frac{N(LS)}{L^n} = \sum_{\underline{x}\in\Lambda_s} \mathbf{1}_{LS}(\underline{x}) = \sum_{\underline{x}\in\frac{1}{L}\Lambda_s} \mathbf{1}_S(\underline{x}) = \sum_{\underline{x}\in\frac{1}{L}\Lambda_s\cap[-B,B]^n} \mathbf{1}_S(\underline{x})$$

is a Riemann sum for the function $\mathbf{1}_S$ on the cube $[-B, B]^n$ by translates of $\left[0, \frac{1}{L}\right]^n$. Since $\mathbf{1}_S$ is Riemann integrable,

$$\lim_{L\to\infty} \frac{N(LS)}{L^n} = \int_{[-B,B]^n} \mathbf{1}_S = \mathrm{vol}(S). \qquad \square$$

Exercise 6.3. Let $S \subseteq \mathbb{R}^n$ be a bounded set such that $\mathbf{1}_S$ is Riemann integrable. Let Λ be a lattice in $\mathbb{R}^n$. Let $N(LS)$ be the cardinality of $LS \cap \Lambda$. Show that

$$\lim_{L\to\infty} \frac{N(LS)}{L^n} = \frac{\mathrm{vol}(S)}{\det(\Lambda)}.$$

6.1. **Another proof of Minkowski's Fundamental Theorem.** We apply Theorem 6.2 to give a different proof of Minkowski's Fundamental Theorem.

Proof. (Second proof of Theorem 3.5) Let $S \subseteq \mathbb{R}^n$ be a bounded, convex, centrally symmetric set such that $\mathrm{vol}(S) > 2^n$. For $L > 0$, let

$N(L)$ be the cardinality of $\frac{L}{2}S \cap \Lambda_s$. By Theorem 6.2 we have

$$\lim_{L\to\infty} \frac{N(L)}{L^n} = \text{vol}\left(\frac{1}{2}S\right) = \frac{\text{vol}(S)}{2^n} > 1.$$

By definition of limit, there exists $L_0 > 0$ such that for $L \geq L_0$ $N(L) > L^n$. Since L^n is the cardinality of $(\mathbb{Z}/L\mathbb{Z})^n$, for $L \geq L_0$ there are at least two distinct points $\underline{x}, \underline{y}$ in $\frac{L}{2}S \cap \Lambda_s$ that have the same residue modulo L (or equivalently the coordinates of $\underline{x}$ and $\underline{y}$ have the same rest after division by L). In particular, $(\underline{x} - \underline{y})/L \in \Lambda_s$. But $(\underline{x} - \underline{y})/2L \in \frac{1}{2}S$, as $\frac{1}{2}S$ is convex and centrally symmetric. Thus $(\underline{x} - \underline{y})/L \in \Lambda_s \cap S$, and $(\underline{x} - \underline{y})/L \neq \underline{0}$ as $\underline{x}$ and $\underline{y}$ are distinct. □

7. Number of lattice points in some unbounded nonconvex sets

A typical nonconvex lattice point counting problem is estimating the cardinality $N(LS)$ of $LS \cap \Lambda_s$, where

$$S = \{(x, y) \in \mathbb{R}^2 : x, y > 0, xy \leq 1\}.$$

Here, the set S is not bounded (and has infinite volume), but $\Lambda_s \cap LS$ is finite for all $L > 0$. Hence, $\Lambda_s \cap LS$ must be contained in a bounded subset S_L of LS. We observe that $1 \leq x, y \leq L$ for all $(x, y) \in \Lambda_s \cap LS$. Let $S_L = LS \cap [1, L]^2$. Then S_L is bounded and $\mathbf{1}_{S_L}$ is Riemann integrable, however we cannot directly apply Theorem 6.2.

Exercise 7.1. Use the strategy of Section 5 to show that $N(LS)$ grows asymptotically like $\text{vol}(S_L)$ as a function of L.

Exercise 7.2. Let

$$S = \{(x, y) \in \mathbb{R}^2 : x, y > 0, x^2y \leq 1\}.$$

Show that $N(LS) = L^3 + O(L^{3/2})$.

References

[CF67] J. W. S. Cassels and A. Fröhlich. *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

[FT93] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[OLD00] C. D. Olds, A. Lax, and G. P. Davidoff. *The geometry of numbers*, volume 41 of *Anneli Lax New Mathematical Library*. Mathematical Association of America, Washington, DC, 2000. Appendix I by Peter D. Lax.

Email address: m.pieropan@uu.nl