AN INTRODUCTION TO THE GEOMETRY OF NUMBERS

NANDANA MADHUKARA

1. Introduction

The study of numbers has long been a central focus of mathematical exploration. From the ancient Greeks to the present day, mathematicians have sought to understand the inherent structures and patterns that underlie the vast realm of numbers. Among the various branches of number theory, the geometry of numbers stands out as a particularly elegant and insightful approach.

This field essentially stems from Hermann Minkowski. Mathematicians during this time were interested in determining whether inequalities had integer solutions. These are called *Diophantine Inequalities*. Mathematicians like Charles Hermite had been using algebraic methods to answer these kinds of questions. Minkowski was also interested in this field but his approach was much different. For example, take the following question that fascinated mathematicians at the time:

Question 1.1. *For any given real number α, are there integers m and n with $m \neq 0$ such that $|\alpha - (n/m)| \leq 1/2m$?*

One way of solving this to take an arbitrary integer $m > 1$ and consider the closest integer n to αm. Then we can just notice

$$|\alpha m - n| \leq \frac{1}{2}$$

so there are an infinite number of pairs of integers m, n that satisfy the inequality. Now Minkowski posed this fact as follows:

Proposition 1.2. *The strip bounded by the straight lines $\alpha x - y = \frac{1}{2}$ and $\alpha x - y = -\frac{1}{2}$ contains infinitely many lattice points.*

These kinds of generalizations to geometry allowed Minkowski to find connections between different problems that other mathematicians didn't notice. He also generalized situations to n-dimensional space which achieved more simple proofs of Hermite's results. Most people consider the pinnacle of the geometry of numbers as Minkowski's famous convex body theorem. This relates "geometric" properties of a set like convexity, symmetry, and volume with "arithmetical" properties like the existence of lattice points in the set. In this paper, we will cover generalizations by Blichfeldt and Minkowski of this result.

2. Preliminaries

2.1. **Lattices.** The main objects we deal with in the geometry of numbers are lattices.

Date: May 28, 2024.

Definition 2.1. Let $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$ be a set of linearly independent vectors in $\mathbb{R}^n$. The set of points

$$\mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$$

for $a_1, a_2, ..., a_n \in \mathbb{Z}$ is called a *lattice* Λ with basis $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$.

Example. When the basis vectors are $\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_n$, we get the familiar lattice points in the $\mathbb{R}^n$ i.e. the set $\{(x_1, ..., x_n) : x_1, ..., x_n \in \mathbb{Z}\}$. We call this lattice Λ_0

We can also take determinants of the lattice.

Definition 2.2. The determinant of a lattice Λ with basis $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$ is

$$d(\Lambda) = |\det(\mathbf{v}_1, ..., \mathbf{v}_n)|$$

where $\det(\mathbf{v}_1, ..., \mathbf{v}_n)$ is the determinant of an $n \times n$ matrix whose ith row is $\mathbf{v}_i$

Notice that this definition is basis independent since every other basis of Λ can be written as $\mathbf{v}_1', \mathbf{v}_2', ..., \mathbf{v}_n'$ where

$$\mathbf{v}_i' = \sum_j a_{ij}\mathbf{v}_j$$

with $\det(a_{ij}) = \pm 1$, so

$$\det(\mathbf{v}_1', ..., \mathbf{v}_n') = \det(a_{ij}) \det(\mathbf{v}_1, ..., \mathbf{v}_n) = \pm \det(\mathbf{v}_1, ..., \mathbf{v}_n).$$

Additionally, since $\mathbf{v}_i$ are linearly independent, we have

$$\det(\Lambda) > 0.$$

2.2. **Lengths.** We can define the length of a vector $\mathbf{v} = (v_1, ..., v_n)$ using the typical definition:

$$|\mathbf{v}| = (v_1^2 + \cdots + v_n^2)^{1/2}.$$

Now let $\mathbf{v} = (v_1, ..., v_n)$ and $\mathbf{u} = (u_1, ..., u_n)$ be two vectors in $\mathbb{R}^n$. Additionally let

$$u_i = \sum_j a_{ij}v_j$$

for $1 \leq i \leq n$ be a real transformation with determinant $\det(a_{ij}) \neq 0$. We now have

$$|\mathbf{u}|^2 = \sum_i \left(\sum_j a_{ij}v_j \right)^2 \leq n^3A^2 \sum_j v_j = n^3A^2|\mathbf{v}|^2$$

where $A = \max_{1 \leq i,j \leq n} |a_{ij}|$. Since $\det(a_{ij}) \neq 0$, the transformation has an inverse so

$$v_i = \sum_j b_{ij}u_j$$

which gives us

$$|\mathbf{v}|^2 \leq n^3B^2|\mathbf{u}|^2$$

where $B = \max_{i,j} |b_{ij}|$. Therefore, there exist constants c_1 and c_2 that depends on the a_{ij}'s and b_{ij}'s such that

$$c_1 \leq \frac{|\mathbf{v}|}{|\mathbf{u}|} \leq c_2.$$

Since the a_{ij}'s and b_{ij}'s can be derived from one another, these constants really only depend on one of the matrices. This leads to the following result:

Lemma 2.3. *Let Λ be a lattice in $\mathbb{R}^n$. Then there exist constants c_1 and c_2 that depend only on Λ and have the following properties*

(1) If $\mathbf{u}, \mathbf{v} \in \Lambda$ and $|\mathbf{u} - \mathbf{v}| < c_1$, then $\mathbf{u}$ and $\mathbf{v}$ are identical.
(2) The number $N(R)$ of points of Λ in the n-ball $|\mathbf{v}| < R$ is at most $c_2 R^n + 1$.

Proof. Notice that for the lattice Λ_0, the first property holds for $c_1 = 1$ and for the second one, we can just crudely bound the n-ball with an n-cube of side length $2R$. This gives us $c_2 = 2^n$. (Of course, there has been a lot of work in finding better bounds). Now for a general lattice Λ in $\mathbb{R}^n$ with basis

$$\mathbf{b}_j = (b_{1j}, ..., b_{nj})$$

where $1 \leq j \leq n$, the points of Λ are $\mathbf{v}$ defined by

$$v_i = \sum_j b_{ij} u_j$$

with $\mathbf{u} \in \Lambda_0$. Therefore, we can bound $|\mathbf{v}|/|\mathbf{u}|$, based off our discussion from before, with constants dependent on the b_{ij}'s (which in turn are dependent on Λ). This means that since the results of lemma hold for Λ_0, the must also hold for Λ. ■

2.3. **Vector Sequences.** Now that we have a metric, we can talk about convergence. We say that a sequence of vectors $(\mathbf{v}_r)_{r \geq 1}$ converges to a vector $\mathbf{v}'$ if

$$\lim_{r \to \infty} |\mathbf{v}_r - \mathbf{v}'| = 0.$$

Clearly, a sufficient and necessary condition is that the coordinates of $\mathbf{v}$ to converge to the coordinates of $\mathbf{v}'$. Now a consequence of Lemma 1 is that a sequence of vectors $\mathbf{v}_r$ in a lattice Λ converge to $\mathbf{v}'$ if there exists an R such that $\mathbf{v}_r = \mathbf{v}'$ for all $r \geq R$.

Definition 2.4. A set of points (or vectors) P is *compact* if every sequence $(\mathbf{v}_r)_{r \geq 1}$ has a subsequence $\mathbf{u}_s = \mathbf{v}_{r_s}$ (where $r_1 < r_2 < \cdots$) that to point in P i.e.

$$\lim_{s \to \infty} y_s = y' \in P.$$

A classic result of Weierstrass is that a set P in $\mathbb{R}^n$ is compact if and only if it is both bounded (contained in a sphere $|\mathbf{v}| < R$ for some sufficiently large R) and closed (the limit of all sequences is in P).

2.4. **Volumes.** In this paper, when we talk about volume we refer to a Lebesgue measure. However, the actual details and properties of this measure will not matter and we will be dealing with sets that have a volume by any definition like cubes and spheres.

3. Blichfeldt's and Minkowski's Theorem

We first start off with the result of Blichfeldt.

Theorem 3.1. *Let m be a positive integer, Λ be a lattice with determinant $d(\Lambda)$, and $\mathcal{P}$ be a set of points in $\mathbb{R}^n$ of volume $V(\mathcal{P})$ (possibly infinite). If*

$$V(P) \geq m \cdot d(\Lambda)$$

and P is compact, there exists $m+1$ distinct points $\mathbf{v}_1$, ..., $\mathbf{v}_{m+1}$ of $\mathcal{P}$ such that all differences $x_i - x_j$ are in Λ.

Proof. Let $\mathbf{b}_0, ..., \mathbf{b}_n$ be a basis of Λ and let $\mathcal{P}_0$ be the generalized parallelopiped

$$y_1\mathbf{b}_1 + \cdots + y_n\mathbf{b}_n$$

where $0 \leq y_i < 1$. This is known as the fundamental parallelopiped for Λ. It's volume is

$$V(\mathcal{P}_0) = |\det(\mathbf{b}_0, ..., \mathbf{b}_n)| = d(\Lambda).$$

Next notice that every point $\mathbf{x} \in \mathbb{R}^n$ can be put in the form $\mathbf{x} = \mathbf{u} + \mathbf{v}$ for $\mathbf{u} \in \Lambda$ and $\mathbf{v} \in \mathcal{P}_0$ and this is unique.

Now for $\mathbf{u} \in \Lambda$ let $\mathcal{R}(\mathbf{u})$ be the set of vectors $\mathbf{v} \in \mathcal{P}_0$ such that $\mathbf{u}+\mathbf{v} \in \mathcal{P}$. Clearly, volumes of $\mathcal{R}(\mathbf{u})$ satisfy

$$\sum_{\mathbf{u}} V(\mathcal{R}(\mathbf{u})) = V(\mathcal{P}).$$

First suppose that $V(\mathcal{P}) > m \cdot d(\Lambda)$. This means that

$$\sum_{\mathbf{u}} V(\mathcal{R}(\mathbf{u})) > m \cdot d(\Lambda) = m \cdot V(\mathcal{P}_0).$$

Now since the $\mathcal{R}(\mathbf{u})$ are contained in $\mathcal{P}$, there must exist a $\mathbf{v}_0 \in \mathcal{P}_0$ that belongs to at least $m+1$ of the $\mathcal{R}(\mathbf{u})$ i.e. $\mathbf{v}_0 \in \mathcal{R}(\mathbf{u}_i)$ where $1 \leq i \leq m+1$ and the $\mathbf{u}_i$ are distinct. This means that the points $\mathbf{x}_j = \mathbf{v}_0 + \mathbf{u}_j$ are in $\mathcal{P}$ by definition and $x_i - x_j = u_i - u_j \in \Lambda$ which proves the theorem.

Next, suppose that $V(\mathcal{P}) = m \cdot d(\Lambda)$. Let $(\varepsilon_r)_{r\geq 1}$ be a sequence of positive numbers with

$$\lim_{r\to\infty} \varepsilon_r = 0.$$

Now we conisder the set of points $(1+\varepsilon_r)\mathcal{P}$ where we scale each point in $\mathcal{P}$ by $1+\varepsilon_r$. This means that

$$V((1+\varepsilon_r)\mathcal{P}) = (1+\varepsilon_r)^n V(\mathcal{P}) > V(\mathcal{P}) = m \cdot d(\Lambda).$$

Therefore, we can use what we have already proven to see that there exist points $\mathbf{x}_{ir} \in (1+\varepsilon_r)\mathcal{P}$ for $1 \leq i \leq m+1$ such that

$$\mathbf{u}_r(i,j) = \mathbf{x}_{ir} - \mathbf{x}_{jr} \in \Lambda.$$

Without loss of generality, let

$$\lim_{r\to\infty} x_{ir} = x_i'$$

for $1 \leq i \leq m+1$. (We can just look at subsequences of ε_r and $\mathbf{x}_{ir}$). Since $\mathcal{P}$ is compact, we know that the $\mathbf{x}_i'$ are in $\mathcal{P}$. Next, we have

$$\mathbf{x}_i' - \mathbf{x}_j' = \lim_{r\to\infty} \mathbf{u}_r(i,j).$$

Now since $\mathbf{u}_r(i,j) \in \Lambda$, there exists an R such that $\mathbf{u}_r(i,j) = \mathbf{u}'(i,j)$ for $r \geq R$. Therefore, we see that $\mathbf{x}_i' - \mathbf{x}_j' = \mathbf{u}'(i,j) \in \Lambda$ so we are done. ∎

From this theorem, we can deduce another result but we first need a definition.

Definition 3.2. A set of points $\mathcal{P}$ is *convex* if every line segment between two points is contained in $\mathcal{P}$. A set is *symmetric* about the origin if $-\mathbf{v} \in \mathcal{P}$ for every $\mathbf{v} \in \mathcal{P}$. A set with both of these properties is called an *M-set*.

Theorem 3.3. *Let $\mathcal{P}$ be an M-set in $\mathbb{R}^n$ of volume $V(\mathcal{P})$ (possibly infinite). Let m be an integer and let Λ be a lattice of determinant $d(\Lambda)$. If*

$$V(\mathcal{P}) \geq m \cdot 2^n \cdot d(\Lambda)$$

and $\mathcal{P}$ is compact, then $\mathcal{P}$ contains at least m different pairs of points $\pm u_i$ (for $1 \leq i \leq m$) which are distinct from the origin $\mathbf{0}$.

Proof. Consider $\frac{1}{2}\mathcal{P}$ which has volume $2^{-n}V(\mathcal{P}) \geq m \cdot d(\Lambda)$. By Theorem 3.1, there exists $m+1$ distinct points $\frac{1}{2}\mathbf{x}_i \in \frac{1}{2}\mathcal{P}$ for $1 \leq i \leq m+1$ such that

$$\frac{1}{2}\mathbf{x}_i - \frac{1}{2}\mathbf{x}_j \in \Lambda.$$

Next, we can order vectors and write $\mathbf{x}_1 > \mathbf{x}_2$ if the first non-zero component of $\mathbf{x}_1 - \mathbf{x}_2$ is positive. Without loss of generality, we can assume

$$\mathbf{x}_1 > \mathbf{x}_2 > \cdots > \mathbf{x}_{m+1}.$$

Let

$$\mathbf{u}_i = \frac{1}{2}\mathbf{x}_i - \frac{1}{2}\mathbf{x}_{m+1}$$

so $\mathbf{0}, \pm\mathbf{u}_1, ..., \pm\mathbf{u}_m$ are all distinct. However, since $\mathcal{P}$ is an M-set and symmetric, we know that $-\mathbf{x}_{m+1} \in \mathcal{P}$ since $\mathbf{x}_{m+1} \in \mathcal{P}$. Therefore, we have

$$\mathbf{u}_i = \frac{1}{2}\mathbf{x}_i + \frac{1}{2}(-\mathbf{x}_{m+1}) \in \mathcal{P}$$

because $\mathcal{P}$ is convex so we are done. ■

A famous corollary of this is when $m = 1$:

Corollary 3.4 (Minkowski's convex body theorem)**.** *An M-set P in $\mathbb{R}^n$ with volume $V(P) \geq 2^n$ contains a point with integral coordinates other than the origin.*

References

[1] H. Minkowski. *Geometrie der Zahlen*. Druck und Verlag von B. G. Teubner., 1910.
[2] C. D. Olds, Anneli Lax, and Giuliana P. Davidoff. *The geometry of numbers*. Mathematical Association of America, 2001.
[3] Cassels J W S. *An introduction to the geometry of numbers*. Springer, 1997.