

SIMULTANEOUS DIOPHANTINE APPROXIMATIONS AND A CONJECTURE OF MINKOWSKI

LENNY FUKSHANSKY

ABSTRACT. This is an introductory expository lecture of elementary level. We start with a brief overview of some classical results in Diophantine approximations, such as Dirichlet's theorem. We then discuss a certain higher dimensional analogue of it, namely approximation of points in a Euclidean space by points of a unimodular lattice. In this direction, we give an overview of the famous conjecture of Minkowski and some of the very exciting recent developments of C. McMullen on this subject.

Recall a classical result from analysis.

Theorem 1. *Rational numbers are dense in reals, i.e. for every two $x < y \in \mathbb{R}$, there exists $\frac{p}{q} \in \mathbb{Q}$ such that*

$$x < \frac{p}{q} < y.$$

Remark 1. Let us agree that we always write rational numbers like $\frac{p}{q}$ in lowest terms, i.e. $\gcd(p, q) = 1$.

The statement of the theorem means that you can approximate any real number arbitrarily well by rational numbers. However this statement is not effective, i.e. it does not tell us anything about the properties of such rational numbers. For instance, given an irrational number α , suppose that we want to approximate it by rational numbers $\frac{p}{q}$ with

$$|q| \leq M$$

for some positive integer M . How closely can we approximate α in this case, and how many such approximations are there? This question is the originating point of the theory of Diophantine approximations. It was first considered by Dirichlet in 1842, who proved the following celebrated theorem.

Theorem 2 (Dirichlet, 1842). *Let $\alpha \in \mathbb{R}$ be an irrational number, and let $M \in \mathbb{Z}_{>0}$. There exist relatively prime integers p, q with $1 \leq q \leq M$ such that*

$$(1) \quad |\alpha q - p| < \frac{1}{M}.$$

Moreover, there are infinitely many rational numbers $\frac{p}{q}$ such that

$$(2) \quad \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Remark 2. The proof of (1) employs the famous Dirichlet box principle, namely the idea that if you have k boxes and $m > k$ objects to put into them, then at least one box must contain at least two objects; in fact, this is the theorem that the principle got its name from. Notice that (2) follows from (1): divide both sides of (1) by q , then we have

$$(3) \quad \left| \alpha - \frac{p}{q} \right| < \frac{1}{Mq} \leq \frac{1}{q^2},$$

since $q \leq M$. Now suppose that there are only finitely many rationals that satisfy (2), call them

$$\frac{p_1}{q_1}, \dots, \frac{p_k}{q_k}.$$

Let

$$\delta = \min_{1 \leq i \leq k} \left| \alpha - \frac{p_i}{q_i} \right|,$$

then $\delta > 0$, since α is irrational. Let $M \in \mathbb{Z}_{>0}$ be such that

$$\frac{1}{M} < \delta.$$

By (3), there must exist $\frac{p}{q}$ with $1 \leq q \leq M$ such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{Mq} < \delta,$$

hence $\frac{p}{q} \notin \left\{ \frac{p_1}{q_1}, \dots, \frac{p_k}{q_k} \right\}$, which is a contradiction. Thus there must be infinitely many such rationals. Notice that this argument is very similar to Euclid's proof of the infinitude of primes.

The famous theorem of K. F. Roth (1955), for which he received a Fields medal in 1958, states that the exponent in (2) is best possible, i.e. if $\frac{1}{q^2}$ in the upper bound is replaced by $\frac{1}{q^e}$ for $e > 2$, then the number of solutions can be finite; in fact, it is finite for every algebraic α .

There is a large variety of higher dimensional generalizations of Dirichlet's theorems. We will consider one of them. We start with some basic notation. Let $N \geq 2$, and let $\mathbf{x}_1, \dots, \mathbf{x}_N \in \mathbb{R}^N$ be linearly

independent vectors. A **lattice** Λ in \mathbb{R}^N spanned by these vectors is the free \mathbb{Z} -module

$$\Lambda = \text{span}_{\mathbb{Z}}\{\mathbf{a}_1, \dots, \mathbf{a}_N\} = \left\{ \sum_{i=1}^N a_i \mathbf{x}_i : a_1, \dots, a_N \in \mathbb{Z} \right\}.$$

Let

$$X = (\mathbf{x}_1 \ \dots \ \mathbf{x}_N)$$

be the corresponding $N \times N$ nonsingular **basis matrix** of Λ . Clearly basis is not unique, hence neither is basis matrix. However, if X and Y are two different basis matrices, then there exists $U \in GL_N(\mathbb{Z})$, the group of all $N \times N$ integral matrices with determinant equal to ± 1 , such that $Y = XU$, and so

$$|\det(Y)| = |\det(XU)| = |\det(X)| |\det(U)| = |\det(X)|.$$

This common value is called **determinant** of Λ , and denoted $\det(\Lambda)$. A lattice Λ is called **unimodular** if $\det(\Lambda) = 1$. The simplest example of a lattice in \mathbb{R}^N is \mathbb{Z}^N ; it is clearly unimodular.

Suppose we have a fixed point $\mathbf{y} \in \mathbb{R}^N$. How closely can we approximate it by points of \mathbb{Z}^N ? Notice that for the purposes of approximation we need a metric. For each $\mathbf{x} \in \mathbb{R}^N$, define

$$\mathcal{N}(\mathbf{x}) = |x_1 \dots x_N|.$$

Notice that this can be thought of as one possible generalization of regular absolute value $|\cdot|$ on \mathbb{R} , in particular it induces a metric of \mathbb{R}^N . Then it is not difficult to see that

$$\sup_{\mathbf{y} \in \mathbb{R}^N} \inf_{\mathbf{x} \in \mathbb{Z}^N} \mathcal{N}(\mathbf{y} - \mathbf{x}) = 2^{-N}.$$

In other words, there exist points in \mathbb{R}^N that cannot be approximated by points of \mathbb{Z}^N better than up to $\frac{1}{2^N}$ with respect to the metric induced by \mathcal{N} . Indeed, if

$$\mathbf{y} = \begin{pmatrix} \frac{1}{2} \\ \vdots \\ \frac{1}{2} \end{pmatrix} \in \mathbb{R}^N,$$

then in fact

$$\inf_{\mathbf{x} \in \mathbb{Z}^N} \mathcal{N}(\mathbf{y} - \mathbf{x}) = \mathcal{N}(\mathbf{y} - \mathbf{0}) = \mathcal{N}(\mathbf{y}) = 2^{-N}.$$

Can we do better if we replace \mathbb{Z}^N with perhaps another unimodular lattice? Minkowski conjectured that at least we will not do any worth.

Define a group of diagonal matrices

$$\mathcal{A} = \left\{ \begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_N \end{pmatrix} : a_i > 0, a_1 \cdots a_N = 1 \right\}.$$

Conjecture 1. *For any unimodular lattice $\Lambda \subset \mathbb{R}^N$, we have:*

$$(4) \quad \sup_{\mathbf{y} \in \mathbb{R}^N} \inf_{\mathbf{x} \in \Lambda} \mathcal{N}(\mathbf{y} - \mathbf{x}) \leq 2^{-N}.$$

Equality holds if and only if there exists $A \in \mathcal{A}$ such that

$$\Lambda = A\mathbb{Z}^N = \text{span}_{\mathbb{Z}}\{a_1\mathbf{e}_1, \dots, a_N\mathbf{e}_N\},$$

where $\mathbf{e}_1, \dots, \mathbf{e}_N$ are the standard basis vectors in \mathbb{R}^N , and $a_1, \dots, a_N \in \mathbb{R}$ are positive with $a_1 \cdots a_N = 1$.

Minkowski's conjecture has been proved for $N = 2$ by Minkowski himself, for $N = 3$ by Remak in 1928, for $N = 4$ by Dyson in 1948, for $N = 5$ by Skubenko in 1976, and for $N = 6$ by McMullen in 2005. We will briefly describe McMullen's exciting approach to this fascinating problem. For this we need some more notation.

For each vector $\mathbf{x} \in \mathbb{R}^N$, write

$$\|\mathbf{x}\| = \left(\sum_{i=1}^N x_i^2 \right)^{1/2}$$

for the usual Euclidean norm of \mathbf{x} . For a lattice $\Lambda \subset \mathbb{R}^N$, define its **covering radius**

$$(5) \quad \mu(\Lambda) = \sup_{\mathbf{y} \in \mathbb{R}^N} \inf_{\mathbf{x} \in \Lambda} \|\mathbf{y} - \mathbf{x}\|.$$

Notice that this is the same expression as in (4), but with respect to $\|\cdot\|$ -norm instead of \mathcal{N} . By the inequality between arithmetic and geometric means, we have

$$(6) \quad \mathcal{N}(\mathbf{x})^{\frac{1}{N}} \leq \frac{\|\mathbf{x}\|}{\sqrt{N}},$$

for all $\mathbf{x} \in \mathbb{R}^N$.

A lattice Λ is called **well-rounded** if there exist N linearly independent vectors in Λ having the same Euclidean norm equal to $\inf_{\mathbf{x} \in \Lambda} \|\mathbf{x}\|$, i.e. all shortest linearly independent vectors of Λ have the same Euclidean norm. The following bound on the covering radius has been proved for well-rounded lattices when $N \leq 6$.

Theorem 3 (Woods, 1972). *Let $N \leq 6$, and let $\Lambda \subset \mathbb{R}^N$ be a well-rounded unimodular lattice. Then*

$$\mu(\Lambda) \leq \frac{\sqrt{N}}{2}.$$

Equality holds if and only if $\Lambda = B\mathbb{Z}^N$ for some $B \in SO_N(\mathbb{R})$.

McMullen, on the other hand, proved that any lattice can be appropriately “rescaled” to a well-rounded one. More specifically, we have the following.

Theorem 4 (McMullen, 2005). *For any lattice $\Lambda \subset \mathbb{R}^N$, there exists $A \in \mathcal{A}$ such that the lattice $A\Lambda$ is well-rounded.*

Now, combining Theorem 4 with (6), (5), and Theorem 3 yields Conjecture 1 for $n \leq 6$. Hence McMullen’s fundamental contribution to Minkowski’s conjecture was the understanding of, if I may say, “distribution” of well-rounded lattices in \mathbb{R}^N .

DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY, TAMU 3368,
COLLEGE STATION, TEXAS 77843-3368

E-mail address: lenny@math.tamu.edu