LECTURE 14: GEOMETRY OF NUMBERS

[NON-EXAMINABLE]

1. Minkowski Convex Body Theorem

Let us consider a (bounded) region D in the n-dimensional space $\mathbb{R}^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{R}\}$. We would like to investigate whether this region contains any points with integral coordinates. This basic geometric problem has numerous applications in Number Theory. Normally, we assume that the domain D is sufficiently nice, so that we can compute its volume $v(D)$.

Our starting point is the following continuous version of the Pigeon-Hole Principle.

Theorem 1.1 (Blichfeldt Principle). *If D is a (bounded) region in $\mathbb{R}^n$ with $v(D) > 1$. then there exist two vectors $v_1 \neq v_2 \in D$ such that $v_1 - v_2 \in \mathbb{Z}^n$.*

For simplicity, we assume that $n = 2$. Essentially the same proof works in any dimension.

Proof. We consider the partition of the plane $\mathbb{R}^2$ into squares:

$$\mathbb{R}^2 = \bigsqcup_{z \in \mathbb{Z}^2} B_z \qquad \text{where} \quad B_z = \{(x_1, x_2) : z_1 \leqslant x_1 < z_1 + 1, z_2 \leqslant x_2 < z_2 + 1\}.$$

Then

$$D = \bigsqcup_{z \in \mathbb{Z}^2} D_z \qquad \text{where} \quad D_z = B_z \cap D.$$

We observe

$$\sum_{z \in \mathbb{Z}^2} v(D_z) = v(D) > 1.$$

Suppose that the sets $D_z - z$, $z \in \mathbb{Z}^2$, are all disjoint. Then since all these sets are contained in B_0, it would follow that

$$\sum_{z \in \mathbb{Z}^2} v(D_z - z) \leqslant v(B_0) = 1.$$

However, $v(D_z - z) = v(D_z)$ and this contradicts the previous estimate. Hence, we conclude that there exists $z_1 \neq z_2 \in \mathbb{Z}^2$ such that

$$(D_{z_1} - z_1) \cap (D_{z_2} - z_2) \neq \emptyset,$$

namely, for some $v_1 \in D_{z_1}$ and $v_2 \in D_{z_2}$, we have $v_1 - z_1 = v_2 - z_2$. This implies the theorem. $\square$

We say that the domain D is *convex* if

$$x_1, x_2 \in D \quad \Rightarrow \quad tx_1 + (1-t)x_2 \in D \text{ for all } t \in [0,1].$$

The domain D is *centrally symmetric* if

$$x \in D \quad \Rightarrow \quad -x \in D.$$

Theorem 1.2 (Minkowski Convex Body Theorem). *Let C be a (bounded) convex centrally symmetric region in $\mathbb{R}^n$ with $v(C) > 2^n$. Then C contains a non-zero integral vector.*

Proof. Let $D = \frac{1}{2}C$. Then $v(D) = \left(\frac{1}{2}\right)^n v(C) > 1$, and we may apply the Blichfeldt Principle. Hence, there exist $v_1 \neq v_2 \in D$ such that $v_1 - v_2 \in \mathbb{Z}^n$. Since

$$v_1 - v_2 = \frac{1}{2}(2v_1) + \frac{1}{2}(-2v_1) \in C,$$

this implies the theorem. $\square$

2. Applications

We prove a version of the Dirichlet Theorem for simultaneous approximation.

Theorem 2.1 (Dirichlet). *Let $\theta_1, \dots \theta_n$ be real numbers. For any integer $Q \geqslant 1$, there exist $p_1, \dots, p_n \in \mathbb{Z}$ and $q = 1, \dots, Q$ such that*

$$\left|\theta_i - \frac{p_i}{q}\right| < \frac{1}{qQ^{1/n}} \quad \textit{for all } i.$$

Proof. We consider the region C in $\mathbb{R}^{n+1}$ defined by

$$-(Q+1) < x_0 < (Q+1), \quad \theta_i x_0 - Q^{-1/n} < x_i < \theta_i x_0 + Q^{-1/n}, \;\; 1 \leqslant i \leqslant n.$$

Since

$$v(C) = 2(Q+1)(2Q^{-1/n})^n > 2^{n+1},$$

it follows from Minkowski's Theorem, there exists nonzero integral vector $z = (q, p_1, \dots, p_n) \in C$. If $q = 0$, then $|p_i| < 1$ and $p_i = 0$ for all i, which is not possible. Hence, $q \neq 0$. Changing z to $-z$ if it is necessary, we can arrange that $q > 0$. This gives the required result. $\square$

Theorem 2.2. *A positive integer is a sum of two squares if and only if it is of the form $p_1^{r_1} \cdots p_s^{r_s}$ where p_i's are primes, and r_i's are even when $p_i \equiv 3 \pmod 4$.*

Proof. Suppose that $x_1^2 + x_2^2 = n$ and a prime $p \equiv 3 \pmod 4$ divides n. If p also divides x_1 and x_2, then also $p^2 | n$. Hence, we obtain $(x_1/p)^2 + (x_2/p)^2 = n/p^2$. On the other hand, x_1 or x_2 is coprime to p, then it follows that the congruence $x^2 \equiv -1 \pmod p$ has solution, but this impossible since $p \equiv 3 \pmod 4$. By induction on n, we deduce that n is of the form $p_1^{r_1} \cdots p_s^{r_s}$ where r_i's are even when $p_i \equiv 3 \pmod 4$.

Let p be a prime such that $p \equiv 1 \pmod 4$. We show that p can be as a sum of two squares. Our assumption on p implies that there exists an integer r such that $r^2 \equiv -1 \pmod p$. We look for solutions of the form

$$p = (pz_1 + rz_2)^2 + z_2^2.$$

We observe that

$$(pz_1 + rz_2)^2 + z_2^2 \equiv (r^2 + 1)z_2^2 \equiv 0 \pmod p. \tag{2.1}$$

We apply the Minkowski Theorem to the ellipsoid

$$C_R = \{(x_1, x_2) : (px_1 + rx_2)^2 + x_2^2 < R^2\}.$$

Since $v(C_{\sqrt{2p}}) = \pi(\sqrt{2p})^2/p > 2^2$, there exists nonzero $(z_1, z_2) \in \mathbb{Z}^2$ such that

$$0 < (pz_1 + rz_2)^2 + z_2^2 < 2p.$$

Because of (2.1), it follows that $(pz_1 + rz_2)^2 + z_2^2 = p$.

The proof of general n follows from the formula

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

□

Theorem 2.3 (Lagrange). *Every positive integer can be written as a sum of four squares.*

Remark 2.4. The congruence $x_1^2 + x_2^2 + x_3^2 \equiv 7 \pmod 8$ has no solutions, so that this theorem is not true for sums of three squares.

Proof. First, we show that every prime p can be written as

$$p = n_1^2 + n_2^2 + n_3^2 + n_4^2.$$

It follows from the Chevalley Theorem that the congruence $u^2 + v^2 + w^2 \equiv 0 \pmod p$ has a non-zero solutions. This implies that there exist $r, s \in \mathbb{Z}$ such that $r^2 + s^2 + 1 \equiv 0 \pmod p$. We shall look for solutions of the form

$$n_1 = pz_1 + rz_3 + sz_4, \quad n_2 = pz_2 + sz_3 - rz_4, \quad n_3 = z_3, \quad n_4 = z_4$$

with $z_1, z_2, z_3, z_4 \in \mathbb{Z}$. We have

$$\begin{aligned} n_1^2 + n_2^2 + n_3^2 + n_4^2 &\equiv (rz_3 + sz_4)^2 + (sz_3 - rz_4)^2 + z_3^2 + z_4^2 \\ &\equiv (r^2 + s^2 + 1)(z_3^2 + z_4^2) \equiv 0 \pmod p. \end{aligned} \tag{2.2}$$

We apply the Minkowski Theorem to the ellipsoid

$$C_R = \{(x_1, x_2, x_3, x_4) : (px_1 + rx_3 + sx_4)^2 + (px_2 + sx_3 - rx_4)^2 + x_3^2 + x_4^2 < R^2\}.$$

A volume computation shows that $v(C_R) = \frac{1}{2}\pi R^4 p^{-2}$. Then

$$v(C_{\sqrt{2p}}) = 2\pi^2 > 2^4,$$

and by the Minkowski Theorem, there exists non-zero $(z_1, z_2, z_3, z_4) \in \mathbb{Z}^4$ such that

$$0 < (pz_1 + rz_3 + sz_4)^2 + (pz_2 + sz_3 - rz_4)^2 + z_3^2 + z_4^2 < 2p.$$

In view of (2.2), we conclude that

$$(pz_1 + rz_3 + sz_4)^2 + (pz_2 + sz_3 - rz_4)^2 + z_3^2 + z_4^2 = p.$$

To give proof for general integers, we use the identity

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) =&(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2\\ &+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ &+(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2\\ &+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2.\end{aligned}$$

$\square$