4

Geometry of numbers

At this stage we require a tool from the Geometry of Numbers, which we shall develop from scratch.

A generalization of the pigeon-hole principle (Schubfachprinzip) says that if we have N things to file in H holes and $N > mH$ for an integer m, then at least one of the holes will contain $\geq (m+1)$ things. We start with a continuous analogue.

Let $\mathbf{R}^n$ denote the vector space of real n-tuples $\mathbf{r} = (r_1, \ldots, r_n)$. It contains the group $\mathbf{Z}^n$ of $\mathbf{r}$ for which $r_j \in \mathbf{Z}$ (all j). By the volume $V(\mathcal{S})$ of a set $\mathcal{S} \subset \mathbf{R}^n$ we shall mean its Lebesgue measure, but in the applications we will be concerned only with very simple-minded $\mathcal{S}$.

Lemma 1. *Let $m > 0$ be an integer and let $\mathcal{S} \subset \mathbf{R}^n$ with*

$$V(\mathcal{S}) > m.$$

Then there are $m+1$ distinct points $\mathbf{s}_0, \ldots, \mathbf{s}_m$ of S such that

$$\mathbf{s}_i - \mathbf{s}_j \in \mathbf{Z}^n \qquad (0 \leq i,\ j \leq m).$$

Proof. Let $\mathcal{W} \subset \mathbf{R}^n$ be the "unit cube" of points $\mathbf{w}$ with

$$0 \leq w_j < 1 \qquad (1 \leq j \leq n).$$

Then every $\mathbf{x} \in \mathbf{R}^n$ is uniquely of the shape

$$\mathbf{x} = \mathbf{w} + \mathbf{z},$$

where $\mathbf{z} \in \mathbf{Z}^n$. Let $\psi(\mathbf{x})$ be the characteristic function of $\mathcal{S}$ ($= 1$ if $\mathbf{x} \in \mathcal{S}$,

$= 0$ otherwise). Then

$$m < V(\mathcal{S}) = \int_{\mathbf{R}^n} \psi(\mathbf{x})d\mathbf{x}$$

$$= \int_{\mathcal{W}} \left(\sum_{\mathbf{z}\in\mathbf{Z}^n} \psi(\mathbf{w}+\mathbf{z}) \right) d\mathbf{w}.$$

Since $V(\mathcal{W}) = 1$, there must be some $\mathbf{w}_0 \in \mathcal{W}$ such that

$$\sum_{\mathbf{z}\in\mathbf{Z}^n} \psi(\mathbf{w}_0+\mathbf{z}) > m,$$

$$\text{so} \quad \geq m+1.$$

We may now take for the $\mathbf{s}_j$ the $\mathbf{w}_0 + \mathbf{z}$ for which $\psi(\mathbf{w}_0+\mathbf{z}) > 0$.

The set $\mathcal{S}$ is said to be *symmetric* (about the origin) if $-\mathbf{x} \in \mathcal{S}$ whenever $\mathbf{x} \in \mathcal{S}$. It is *convex* if whenever $\mathbf{x}, \mathbf{y} \in \mathcal{S}$, then the whole line-segment

$$\lambda\mathbf{x} + (1-\lambda)\mathbf{y} \in \mathcal{S} \qquad (0 \leq \lambda \leq 1)$$

joining them is in $\mathcal{S}$. In particular, the mid-point $\frac{1}{2}(\mathbf{x}+\mathbf{y})$ is in $\mathcal{S}$.

Theorem 1. *Let Λ be a subgroup of $\mathbf{Z}^n$ of index m. Let $\mathcal{C} \subset \mathbf{R}^n$ be a symmetric convex set of volume*

$$V(\mathcal{C}) > 2^n m.$$

Then $\mathcal{C}$ and Λ have a common point other than $\mathbf{0} = (0,\ldots,0)$.

Proof. Let $\mathcal{S} = \frac{1}{2}\mathcal{C}$ be the set of points $\frac{1}{2}\mathbf{c}$, $\mathbf{c} \in \mathcal{C}$. Then

$$V(\tfrac{1}{2}\mathcal{C}) = 2^{-n}V(\mathcal{C}) > m.$$

By Lemma 1, there are $m+1$ distinct points $\mathbf{c}_0, \ldots, \mathbf{c}_m \in \mathcal{C}$ such that

$$\tfrac{1}{2}\mathbf{c}_i - \tfrac{1}{2}\mathbf{c}_j \in \mathbf{Z}^n . \quad (0 \leq i,\ j \leq m).$$

There are $m+1$ points

$$\tfrac{1}{2}\mathbf{c}_i - \tfrac{1}{2}\mathbf{c}_0 \qquad (0 \leq i \leq m)$$

and m cosets of $\mathbf{Z}^n$ modulo Λ. By the pigeon hole principle, two must be in the same coset, that is there are i, j with $i \neq j$ such that

$$\tfrac{1}{2}\mathbf{c}_i - \tfrac{1}{2}\mathbf{c}_j \in \Lambda.$$

Now $-\mathbf{c}_j \in \mathcal{C}$ by symmetry; and so

$$\tfrac{1}{2}\mathbf{c}_i - \tfrac{1}{2}\mathbf{c}_j = \tfrac{1}{2}\mathbf{c}_i + \tfrac{1}{2}(-\mathbf{c}_j) \in \mathcal{C}$$

by convexity.

Note. Lemma 1 and Theorem 1 with $m = 1$ are due to Blichfeldt and Minkowski respectively. The generalizations to $m > 1$ are by van der Corput.

As a foretaste of the flavour of the application in the next section, we give

Lemma 2. *Let N be a positive integer. Suppose that there is an $l \in \mathbf{Z}$ such that*

$$l^2 \equiv -1 \ (N).$$

Then $N = u^2 + v^2$ for some $u, v \in \mathbf{Z}$.

Proof. We take $n = 2$ and denote the co-ordinates by x, y. For $\mathcal{C}$ we take the open disc

$$x^2 + y^2 < 2m$$

of volume (= area)

$$V(\mathcal{C}) = 2\pi m > 2^2 m.$$

The subgroup Λ of $\mathbf{Z}^2$ is given by

$$x, y \in \mathbf{Z}, \qquad y \equiv lx \ \ (m).$$

It is clearly of index m. Hence by the Theorem there is

$$(0,0) \neq (u,v) \in \Lambda \cap \mathcal{C}.$$

Then

$$0 < u^2 + v^2 < 2m$$

and

$$u^2 + v^2 \equiv u^2(1 + l^2) \equiv 0 \ \ (m).$$

Hence $u^2 + v^2 = m$, as required.

We note, in passing, that the condition of the lemma is certainly satisfied for primes p with $p \equiv 1 \ (4)$.

§4. Exercises

1. Let $m \in \mathbf{Z}$, $m > 1$ and suppose that there is some $f \in \mathbf{Z}$ such that $f^2 + f + 1 \equiv 0 \ (m)$. Show that $m = u^2 + uv + v^2$ for some $u, v \in \mathbf{Z}$.

2. Find a prime $p > 0$ for which there is an $f \in \mathbf{Z}$ such that

$$1 + 5f^2 \equiv 0 \ (p)$$

but p is not of the shape $u^2 + 5v^2$ $(u, v \in \mathbf{Z})$.