ON A THEOREM OF MINKOWSKI'S

A. C. WOODS

Let K be a closed strictly convex body in R_n symmetric in the origin 0. Let Λ be a K-admissible lattice, i.e. apart from 0 no point of Λ is in the interior of K. A theorem of Minkowski's (1) is that there are at most 2^n-1 pairs of points $\pm X$ of Λ that lie on the boundary of K. I note here that this is a special case of a theorem which applies to any lattice.

Let K be as above and let Λ be an arbitrary lattice in R_n, so not necessarily K-admissible. The n numbers $\mu_1(\Lambda), \mu_2(\Lambda), \cdots, \mu_n(\Lambda)$, called the successive minima of Λ with respect to K, are defined as the least upper bounds respectively of numbers $c_1, c_2, \cdots, c_n$ with the property that c_iK contains at most $i-1$ linearly independent points of Λ within its interior. Let $X_1, X_2, \cdots, X_n$ be n linearly independent points of Λ such that $\mu_i(\Lambda)K$ contains $X_1, X_2, \cdots, X_i$ for $i=1, 2, \cdots, n$. Let $Z_1, Z_2, \cdots, Z_n$ be a basis of Λ such that

$$X_i = \sum_{j=1}^{i} g_{ij}Z_j \qquad (i = 1, 2, \cdots, n)$$

where the coefficients g_{ij} are integers with $g_{ii}>0$. Denote by $X_{i1}, X_{i2}, \cdots, X_{ir_i}$ all the points of $\Lambda \cap \mu_i(\Lambda)K$ of the form

$$X_{is} = \sum_{j=1}^{i} g_{ij}^{(s)} Z_j$$

where the coefficients $g_{ij}^{(s)}$ are integers with $g_{ii}^{(s)}>0$. Then we have the result

THEOREM. $\sum_{i=1}^{n} r_i \leqq 2^n-1$.

PROOF. Take coordinates such that $Z_1, Z_2, \cdots, Z_n$ are the points $(1, 0, 0, \cdots, 0), (0, 1, 0, \cdots, 0), \cdots, (0, 0, \cdots, 0, 1)$ respectively. Then Λ is the set of points with integral coordinates. We say that two points of Λ are congruent modulo 2 if the corresponding differences between their coordinates are divisible by 2. From the definition of the successive minima of Λ it follows that every one of the points X_{is} is primitive and therefore in particular no one of them is congruent to $0=(0, 0, \cdots, 0)$ modulo 2. We assert that no two of these points can be congruent modulo 2. For assume that this assertion is false. Then for two distinct pairs of indices i, s and i', s'

Received by the editors November 25, 1957.

the points X_{is} and $X_{i's'}$ are congruent modulo 2. Hence $(X_{is}+X_{i's'})/2$ and $(X_{is}-X_{i's'})/2$ are points of Λ. If $(X_{is}+X_{i's'})/2=X_{is}$ then $X_{is}=X_{i's'}$ which is impossible since by definition distinct pairs of suffixes yield distinct points, therefore $(X_{is}+X_{i's'})/2\neq X_{is}$. Similarly $(X_{is}+X_{i's'})/2\neq X_{i's'}$. If $(X_{is}-X_{i's'})/2=X_{is}$ then $X_{is}=-X_{i's'}$ and therefore in particular $i=i'$. Hence $g_{tt}^{(s)}=-g_{t't'}^{(s')}$, but as $g_{tt}^{(s)}$ and $g_{tt}^{(s')}$ are positive integers this is impossible, hence $(X_{is}-X_{i's'})/2\neq X_{is}$. Similarly $(X_{is}-X_{i's'})/2\neq -X_{i's'}$. There is no loss of generality in assuming that $i\geqq i'$. It follows that X_{is} and $X_{i's'}$ are contained in $\mu_i(\Lambda)K$. From the strict convexity of K it follows that $(X_{is}+X_{i's'})/2$ and $(X_{is}-X_{i's'})/2$ are in the interior of $\mu_i(\Lambda)K$. Now

$$X_{is} = (X_{is} + X_{i's'})/2 + (X_{is} - X_{i's'})/2$$

so that X_{is} is linearly dependent on two points of Λ which lie in the interior of $\mu_i(\Lambda)K$. As this is impossible the assertion is proved. The assertion implies that no two of the points X_{is} can lie in the same residue class modulo 2 and since as we have already seen no one of these points is congruent to 0 modulo 2 it follows that there are at most 2^n-1 such points and the theorem is proved.

Minkowski extended his result to convex bodies which are not strictly convex by showing that if Λ is an admissible lattice of an arbitrary convex body K symmetric in the origin then there are at most 3^n-1 points of Λ on the boundary of K. Here the extension breaks down for let K be a convex body symmetric in the origin such that the boundary of K contains a line segment. Take coordinates so that one such line segment has the endpoints $(1, 1, 0, \cdots, 0)$, $(-1, 1, 0, \cdots, 0)$. For an arbitrary pair of positive integers M, N denote by $\Lambda(M, N)$ the lattice generated by the point $(N^{-1}, 0, 0, \cdots, 0)$, $(0, 1, 0, \cdots, 0)$, $(0, 0, M, 0, \cdots, 0), \cdots,$ $(0, 0, \cdots, 0, M)$. As K is bounded so for all sufficiently large values of M, $r_1=1$ and $r_2\geqq 2N+1$ whence $\sum_{t+1}^{n} r_i\geqq 2N+2$ which tends to infinity with N.

Reference

1. H. Minkowski, *Geometrie der Zahlen*, Leipzig, 1928.

Tulane University of Louisiana