Annals of Mathematics
Vol. 48, No. 4, October, 1947

EXISTENCE THEOREMS IN THE GEOMETRY OF NUMBERS

By C. A. Rogers

(Received December 4, 1946)

1. A fundamental theorem[1] of Minkowski states that if $\mathfrak{G}$ is a lattice of determinant Δ in n dimensional space, and K is a convex body, symmetrical about the origin O, whose volume $V(K)$ satisfies

$$V(K) > 2^n\Delta,$$

then K contains a point of $\mathfrak{G}$ other than O. Thus, if $\Delta(K)$ denotes the lower bound of the determinants Δ of the lattices $\mathfrak{G}$ with only the point O in K, Minkowski's result is equivalent to the inequality

$$\Delta(K) \geqq 2^{-n}V(K), \tag{1}$$

for all convex bodies K, symmetrical about O. On the other hand Minkowski[2] asserted that, if S is an n-dimensional star body, symmetrical about the origin O, with volume less than

$$2\zeta(n) = 2\left\{1 + \frac{1}{2^n} + \frac{1}{3^n} + \cdots\right\},$$

then there exists a lattice $\mathfrak{G}$ of determinant 1 such that O is the only point of $\mathfrak{G}$ in S. This implies that for every symmetrical star body S,

$$\Delta(S) \leqq \frac{V(S)}{2\zeta(n)}. \tag{2}$$

Minkowski[3] gave a rather difficult proof of his assertion in the particular case when S is a sphere, but he never published a general proof.

Blichfeldt[4] stated that he had proved a slightly better result when S is a convex body, but apparently he did not publish his proof. Mahler[5] has published a proof of a slightly weaker form of Minkowski's assertion. The first complete proof was given by Hlawka,[6] who proved the following theorem, and who was able to deduce Minkowski's assertion as a consequence.

Theorem 1. *Suppose $\rho(P)$ is a function of the coordinates of the point P in the n-dimensional Euclidean space Ω. Suppose $\rho(P)$ is bounded and integrable*

---

[1] See, for example, G. H. Hardy and E. M. Wright, *The theory of numbers*, (Oxford, 1945).

[2] H. Minkowski, *Gesammelte Abhandlungen* (Leipzig, 1911), vol. 1, 265, 270 and 277.

[3] H. Minkowski, *Loc. cit*, vol. 2, 94–95.

[4] H. F. Blichfeldt, *Report of the Geometry of Numbers*, Amer. Math. Soc. Bull, **25** (1919), 449–453 (451). See also B. A. Bernstein, *Meeting of the San Francisco Section*, Amer. Math. Soc. Bull., **24** (1918), 417–420 (418).

[5] K. Mahler, *On a theorem of Minkowski*, London Math. Soc. Jour., **19** (1944), 201–205. This paper is independent Hlawka's work, but it appeared just after Hlawka's paper.

[6] E. Hlawka, *Zur Geometrie der Zahlen*, Math. Zeitschr., **49** (1944), 285–312.

in the Riemann sense throughout Ω and vanishes outside a bounded region in Ω. Then for any $\epsilon > 0$, there exists a lattice $\mathfrak{G}$ of determinant 1 such that

$$\sum{}' \rho(G) \leqq \int_\Omega \rho(P)\, dP + \epsilon, \tag{3}$$

the summation[7] *extending over all the points G of the lattice $\mathfrak{G}$ other than the origin O.*

Siegel[8] has recently given another proof of Minkowski's assertion. He gives a proof of Theorem 1 which shows that the conclusion remains true when ϵ is taken to be zero. Then by a modification of his argument he proves that, under the same hypotheses, there exist a lattice $\mathfrak{G}$ of determinant 1 such that

$$\sum{}^* \rho(G) \leqq \frac{1}{\zeta(n)} \int_\Omega \rho(P)\, dP, \tag{4}$$

where the summation extends over the set $\mathfrak{G}^*$ of primitive points of the lattice $\mathfrak{G}$. He shows that Minkowski's assertion is an immediate consequence of this result. Siegel also indicates a number of directions in which the results can be generalized.

In this paper a simple proof of Hlawka's theorem (Theorem 1) is given. The method of proof will be modified to establish Theorem 2, which is the theorem of Siegel just mentioned, except for an ϵ term. This theorem will be used to deduce Minkowski's assertion and to prove a new theorem (Theorem 3) on the successive minima associated with a lattice and a star body. This third theorem, which is a partial converse of Minkowski's generalized inequality will be used to establish the following result.

THEOREM 4. *There exists a positive definite quadratic form Q of unit determinant in n variables, $u_1, u_2, \cdots, u_n$, say, such that*

$$Q \geqq \frac{1}{\pi}\left(\frac{2n\zeta(n)}{e(1 - e^{-n})}\right)^{2/n} (\Gamma(1 + \tfrac{1}{2}n))^{2/n}, \tag{5}$$

for all sets $(u_1, u_2, \cdots, u_n)$ of integral values of the variables, other than the set $(0, 0, \cdots, 0)$.

2. PROOF OF THEOREM 1. For simplicity it will be assumed in the first place that $\rho(P)$ is non-negative. Later it will be shown that the theorem is true in general.

Let p be a large prime and write $q = p^{n-1}$. Let $\mathfrak{L}$ denote the lattice of all points with integral coordinates. Let $A_1, A_2, \cdots, A_q$ be the points of $\mathfrak{L}$ whose coordinates satisfy

$$x_1 = 1,$$
$$0 \leqq x_r < p, \qquad \text{for } r = 2, 3, \cdots, n.$$

[7] Throughout this paper a capital italic letter is used to denote a typical point of the set denoted by the corresponding German letter. Σ' is used to denote a summation extending over all the points, other than O, of the appropriate set, and Σ^* will be used to denote a summation extending over all the primitive points of the set.

[8] C. L. SIEGEL, *Geometry of Numbers*, Annals of Math., 46 (1945), 340–347.

If C is any point of $\mathfrak{L}$, with coordinates $(c_1, c_2, \cdots, c_n)$, for which

$$c_1 \not\equiv 0 \pmod{p},$$

the congruences

$$u \equiv c_1 \pmod{p},$$

$$ux_r \equiv c_r \pmod{p}, \qquad \text{for } r = 2, 3, \cdots, n,$$

have a unique solution for the integers $u, x_2, x_3, \cdots, x_n$, subject to the inequalities

$$1 \leqq u < p,$$

$$0 \leqq x_r < p, \qquad \text{for } r = 2, 3, \cdots, n.$$

So, if $\mathfrak{C}$ is the set of all points C of $\mathfrak{L}$, for which $c_1 \not\equiv 0 \pmod{p}$, every point C of $\mathfrak{C}$ is representable uniquely in the form $uA_i + pL$, where $1 \leqq u < p$ and $1 \leqq i < q$ and L is a point of $\mathfrak{L}$. In this way, the set $\mathfrak{C}$ is divided into q classes $\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_q$; the class $\mathfrak{B}_i$ being the set of points B_i, whose representation involves A_i.

As $\rho(P)$ is integrable in the Riemann sense,

$$\lim_{p \to \infty} p^{-(n-1)} \sum{}' \rho(p^{(1/n)-1} \cdot L) = \int_\Omega \rho(P)\, dP.$$

Thus, for any $\epsilon > 0$, if p is sufficiently large,

$$\sum{}' \rho(p^{(1/n)-1} \cdot L) < q\left\{\int_\Omega \rho(P)\, dP + \epsilon\right\}. \tag{6}$$

Using the assumption that $\rho(P)$ is non-negative, this implies that

$$\sum \rho(p^{(1/n)-1} \cdot C) < q\left\{\int_\Omega \rho(P)\, dP + \epsilon\right\}. \tag{7}$$

So, for one class, say $\mathfrak{B}$, of the q classes $\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_q$, which together make up $\mathfrak{C}$, we have

$$\sum \rho(p^{(1/n)-1} \cdot B) < \int_\Omega \rho(P)\, dP + \epsilon,$$

the sum extending over all the points B of $\mathfrak{B}$.

Suppose A is the point A_i corresponding to the class $\mathfrak{B}$, and consider the lattice $\mathfrak{G}$ of points generated by the point $p^{(1/n)-1} \cdot A$ and the points with coordinates

$$\begin{gathered}(0, p^{1/n}, 0, \cdots, 0),\\ (0, 0, p^{1/n}, \cdots, 0),\\ \cdots\\ (0, 0, 0, \cdots, p^{1/n}).\end{gathered}$$

Every point G of $\mathfrak{G}$ is of the form

$$G = p^{(1/n)-1}\{uA + pL\},$$

where u is an integer and L is a point of $\mathfrak{L}$. If $u \equiv 0 \pmod{p}$, the point G is of the form $p^{1/n}\cdot L$ where L is a point of $\mathfrak{L}$, and conversely every such point is a point of $\mathfrak{G}$. If $u \not\equiv 0 \pmod{p}$, the point G is of the form $p^{(1/n)-1}\cdot B$ where B is a point of $\mathfrak{B}$, and again every such point is a point of $\mathfrak{G}$. Thus

$$\sum{}' \rho(G) = \sum{}' \rho(p^{1/n}\cdot L) + \sum \rho(p^{(1/n)-1}\cdot B).$$

But $\rho(P)$ vanishes outside a bounded region, so that

$$\sum{}' \rho(p^{1/n}\cdot L) = 0,$$

if p is sufficiently large. Then

$$\sum{}' \rho(G) < \int_{\Omega} \rho(P)\, dP + \epsilon.$$

The determinant of $\mathfrak{G}$ being 1, this proves the required result when $\rho(P)$ is non-negative.

The only stage in this proof, where the assumption that $\rho(P)$ is non-negative has been used, is the deduction of the inequality (7) from the inequality (6). Consider the difference

$$\sum \rho(p^{(1/n)-1}\cdot C) - \sum{}' \rho(p^{(1/n)-1}\cdot L).$$

The only contributions to the difference come from the points of the set $\mathfrak{D}$ of all points D of $\mathfrak{L}$ for which $d_1 \equiv 0 \pmod{p}$; so that

$$\sum \rho(p^{(1/n)-1}\cdot C) - \sum{}' \rho(p^{(1/n)-1}\cdot L) = -\sum{}' \rho(p^{(1/n)-1}\cdot D).$$

Since $\rho(P)$ vanishes outside a bounded region, if p is sufficiently large, the only contributions to the sum on the right hand side come from the points of $\mathfrak{D}$ for which $d_1 = 0$. As $\rho(P)$ is bouned, it follows that, as p tends to infinity,

$$-\sum \rho(p^{(1/n)-1}\cdot D) = O(p^{[1-(1/n)](n-1)}) = o(p^{n-1}).$$

Thus, if p is sufficiently large the inequality (6) implies the inequality obtained from (7) by writing 2ϵ for ϵ.

Corollary. *If S is any bounded set of points, symmetrical about O, with volume $V(S)$, satisfying*

$$V(S) < 2,$$

it is possigle to find a lattice $\mathfrak{G}$ of unit determinant, which has no point in S, except possibly O.

To prove this corollary one has merely to consider the function, defined by

$$\rho(P) = \tfrac{1}{2}, \text{ if } P \text{ is in } S, \text{ and}$$
$$\rho(P) = 0, \text{ if } P \text{ is not in } S,$$

and to notice that, if a symmetrical set contains a lattice point G, other than 0, it also contains the lattice point $-G$.

3. In this section we show how the proof of Theorem 1 can be modified to establish the following theorem.

THEOREM 2. *Suppose $\rho(P)$ is a function of the coordinates of the point P in the n-dimensional Euclidean space Ω. Suppose $\rho(P)$ is bounded and integrable in the Riemann sense throughout Ω and vanishes outside a bounded region in Ω. Then, for any $\epsilon > 0$, there exists a lattice $\mathfrak{G}$ of determinant 1 such that*

$$\sum{}^{*} \rho(G) \leqq \frac{1}{\zeta(n)} \int_\Omega \rho(P)\, dP + \epsilon,$$

the summation extending over the set $\mathfrak{G}^*$ of primitive lattice points of $\mathfrak{G}$.

We first prove the following lemma.

LEMMA. *If $\rho(P)$ satisfies the conditions of Theorem 2, then*

$$\lim_{\lambda \to +0} \lambda^n \sum{}^{*} \rho(\lambda L) = \frac{1}{\zeta(n)} \int_\Omega \rho(P)\, dP,$$

the summation extending over the set $\mathfrak{L}^*$ of primitive points of the lattice $\mathfrak{L}$ of points with integral coordinates.

PROOF OF LEMA. For all $\lambda > 0$,

$$\sum{}' \rho(\lambda L) = \sum_{r=1}^{\infty} \sum{}^{*} \rho(r\lambda L),$$

and, as $\rho(P)$ vanishes ouside a bounded region, the sum on the right hand side has only a finite number of non-zero terms. Applying the Möbius inversion formula, for all $\lambda > 0$,

$$\sum{}^{*} \rho(\lambda L) = \sum_{r=1}^{\infty} \mu(r) \sum{}' \rho(r\lambda L).$$

Thus

$$\lambda^n \sum{}^{*} \rho(\lambda L) = \sum_{r=1}^{\infty} \mu(r) r^{-n} (r\lambda)^n \sum{}' \rho(r\lambda L).$$

Now $| (r\lambda)^n \sum{}' \rho(r\lambda L) |$ is bounded for all positive values of r and λ, and for each fixed value of r

$$\lim_{\lambda \to +0} (r\lambda)^n \sum{}' \rho(r\lambda L) = \int_\Omega \rho(P)\, dP.$$

So

$$\lim_{\lambda \to +0} \lambda^n \sum{}^{*} \rho(\lambda L) = \sum_{r=1}^{\infty} \mu(r) r^{-n} \int_\Omega \rho(P)\, dP$$

$$= \frac{1}{\zeta(n)} \int_\Omega \rho(P)\, dP.$$

PROOF OF THEOREM 2. Assume in the first place that $\rho(P)$ is a non-negative function. The points C of the set $\mathfrak{C}$ of points of $\mathfrak{L}$, whose first coordinate is not congruent to zero mod. p, are divided, as before, into classes $\mathfrak{B}_1, \mathfrak{B}_2, \cdots,$

$\mathfrak{B}_q$. Let $\mathfrak{B}_i^*$ denote the set of points of $\mathfrak{B}_i$ which are primitive points of $\mathfrak{L}$. The sets $\mathfrak{B}_1^*, \mathfrak{B}_2^*, \cdots, \mathfrak{B}_q^*$ then make up the set $\mathfrak{C}^*$ of primitive points of $\mathfrak{C}$.

We prove that a point B of $\mathfrak{B}_i$ is in $\mathfrak{B}_i^*$ if, and only if, there is no point of $\mathfrak{B}_i$ between O and B on the segment OB. It is obvious that, if there is such a point of $\mathfrak{B}_i$, then B is not a primitive point of $\mathfrak{L}$, and so is not in $\mathfrak{B}_i^*$. Conversely, if B is in $\mathfrak{B}_i$, but is not in $\mathfrak{B}_i^*$ then there is a point D say, of $\mathfrak{L}$ on OB between O and B. We may suppose, without loss of generality, that

$$B = nD,$$

where n is a positive integer. We prove that D is a point of $\mathfrak{B}_i$. As

$$b_1 \not\equiv 0 \pmod{p},$$

clearly

$$n \not\equiv 0 \pmod{p}.$$

Suppose

$$B = uA_i + pL,$$

where u is an integer, satisfying $0 < u < p$ and L is some point of $\mathfrak{L}$; and suppose m is the solution of the congruence

$$nm \equiv 1 \text{ (mod. } p).$$

Then

$$\begin{aligned} D &= mnD - (nm - 1)D \\ &= muA_i + mpL - (nm - 1)D. \end{aligned}$$

As $u \not\equiv 0$ (mod. p) and $m \not\equiv 0$ (mod. p) it follows that $mu \not\equiv 0$ (mod. p), and D is a point of $\mathfrak{B}_i$ between O and B on the segment OB.

The lemma shows that

$$\lim_{p \to \infty} p^{-(n-1)} \sum{}^* \rho(p^{(1/n)-1} \cdot L) = \frac{1}{\zeta(n)} \int_\Omega \rho(P)\, dP.$$

Thus, for any $\epsilon > 0$, if p is sufficiently large,

$$\sum{}^* \rho(p^{(1/n)-1} \cdot L) < q \left\{ \frac{1}{\zeta(n)} \int_\Omega \rho(P)\, dP + \epsilon \right\}.$$

As $\rho(P)$ has been assumed to be non-negative, this implies that for one of the classes $\mathfrak{B}_1^*, \mathfrak{B}_2^*, \cdots, \mathfrak{B}_q^*$, say $\mathfrak{B}^*$, we have

$$\sum{}^* \rho(p^{(1/n)-1} \cdot B) < \frac{1}{\zeta(n)} \int_\Omega \rho(P)\, dP + \epsilon.$$

The lattice $\mathfrak{G}$ can now be defined as before. To complete the proof in the case when $\rho(P)$ is non-negative it is only necessary to notice that the set $\mathfrak{G}^*$

of primitive points of the lattice $\mathfrak{G}$, consists of the points of the form $p^{(1/n)-1} \cdot B$, where B is in $\mathfrak{B}^*$, together with certain points of the form $p^{1/n} \cdot L$, where L is in $\mathfrak{L}^*$. The restriction that $\rho(P)$ is non-negative can be removed as before.

Corollary. *If S is any bounded star body, symmetrical about O, with a volume $V(S)$, satisfying*

$$V(S) < 2\zeta(n),$$

it is possible to find a lattice $\mathfrak{G}$ of unit determinant such that O is the only point of $\mathfrak{G}$ in S.

It follows immediately from recent work of Mahler[9] that, if S satisfies a certain continuity condition, the word "bounded" can be omitted from this corollary. If in addition S is assumed to be open, the sign of inequality can be replaced by one of equality.

4. Suppose S is any bounded closed star body, and $\mathfrak{G}$ is a lattice. We define λ_1 to be the least value of λ such that the body λS contains some point, P_1 say, of $\mathfrak{G}$ other than O. The successive minima $\lambda_2, \lambda_3, \cdots, \lambda_n$ are defined so that, for $r = 1, 2, \cdots, n - 1$, the number λ_{r+1} is the least value of λ such that the body λS contains some point, P_{r+1} say, which is linearly independent of $P_1, P_2, \cdots, P_r$. The numbers $\lambda_1, \lambda_2, \cdots, \lambda_n$ defined in this way are called the successive minima of S for $\mathfrak{G}$.

Theorem 3. *If S is any closed bounded star body, symmetrical about the origin O, with volume $V(S)$, satisfying*

$$V(S) < \frac{2n\zeta(n)}{e(1 - e^{-n})}, \tag{8}$$

it is possible to find a lattice $\mathfrak{G}$ of unit determinant such that

$$\lambda_1\lambda_2\lambda_3 \cdots \lambda_n > 1,$$

where $\lambda_1, \lambda_2, \cdots, \lambda_n$ are the successive minima of S for $\mathfrak{G}$.

Proof. We may suppose that S is the set of points P satisfying

$$f(P) \leqq 1,$$

where $f(P)$ is a non-negative function satisfying the functional equation

$$f(\lambda P) = |\lambda| \cdot f(P),$$

for all points P and all real numbers λ. Consider the non-negative function $\rho(P)$, defined by

$$\begin{aligned} \rho(P) &= 1 , && \text{if } 0 \leqq f(P) \leqq e^{(1/n)-1}, \\ \rho(P) &= (1/n) - \log f(P), && \text{if } e^{(1/n)-1} \leqq f(P) \leqq e^{1/n} \text{ and} \\ \rho(P) &= 0 , && \text{if } e^{1/n} \leqq f(P). \end{aligned}$$

[9] K. Mahler, *On lattice points in star bodies*, Roy. Soc. London, Proc., A **187** (1946), 151–187 (151–162).

Now the integral

$$\int_\Omega \rho(P)\, dP$$

may be regarded as the mass of a star body of varying density $\rho(P)$. By splitting this body up into shells such as that defined by

$$\mu < f(P) \leqq \mu + \delta\mu,$$

it is easy to see that

$$\int_\Omega \rho(P)\, dP = \int_0^a V(S) n\mu^{n-1}\, d\mu + \int_a^b \left(\frac{1}{n} - \log \mu\right) V(S) n\mu^{n-1}\, d\mu,$$

where $a = e^{(1/n)-1}$ and $b = e^{1/n}$. Evaluating the integrals, we have

$$\int_\Omega \rho(P)\, dP = \frac{e}{n}(1 - e^{-n}) V(S) < 2\zeta(n).$$

By Theorem 2 it is possible to find a lattice $\mathfrak{G}$ of unit determinant such that

$$\sum{}^* \rho(G) < 2.$$

Now, using the notation of the definition, the points $\pm P_1, \pm P_2, \cdots, \pm P_n$ are primitive points of $\mathfrak{G}$ and are on the surfaces of the bodies $\lambda_1 S, \lambda_2 S, \cdots, \lambda_n S$. Thus

$$2 \sum_{r=1}^{n} \rho(P_r) < 2.$$

This shows that none of the points $P_1, P_2, \cdots, P_n$ can be such that $f(P) < a$, and consequently

$$\rho(P_r) \geqq (1/n) - \log \lambda_r, \text{ for } r = 1, 2, \cdots, n.$$

So

$$-\sum_{r=1}^{n} \log \lambda_r \leqq \left(\sum_{r=1}^{n} \rho(P_r)\right) - 1 < 0,$$

and

$$\lambda_1 \lambda_2 \lambda_3 \cdots \lambda_n > 1.$$

5. Proof of Theorem 4. Let γ be any number such that

$$\gamma^2 < \frac{1}{\pi}\left(\frac{2n\zeta(n)}{e(1 - e^{-n})}\right)^{2/n} (\Gamma(1 + \tfrac{1}{2} n))^{2/n}. \tag{9}$$

Consider the sphere S of radius γ and volume

$$\frac{\pi^{n/2}}{\Gamma(1 + \frac{1}{2}n)} \gamma^n < \frac{2n\zeta(n)}{e(1 - e^{-n})}.$$

By Theorem 3, there exists a lattice $\mathfrak{G}$ of unit determinant such that the successive minima of S for $\mathfrak{G}$ satisfy

$$\lambda_1\lambda_2\lambda_3 \cdots \lambda_n > 1.$$

This means that there exists a positive definite quadratic form Q of unit determinant, such that the product

$$S_1S_2S_3 \cdots S_n$$

of its successive minima is greater than γ^{2n}. But Minkowski[10] has proved, by a simple argument, that in such a case, there exists another positive definite quadratic form Q^* of unit determinant and minimum $M^* > \gamma^2$. As this is true for all numbers γ satisfying (9), it follows from the work of Mahler[11] that there exists a positive definite quadratic form of unit determinant, with minimum greater than or equal to

$$\frac{1}{\pi}\left(\frac{2n\zeta(n)}{e(1 - e^{-n})}\right)^{2/n} (\Gamma(1 + \tfrac{1}{2}n))^{2/n}.$$

I am grateful to Professor Davenport, who has advised me during the construction of the proofs of these theorems.

(*Note added, 30 July, 1947.* In a recent paper (Duke Math. Jour., **13** (1946), 611–621.) Dr. Mahler has proved, in particular, that for every convex body K, symmetrical about O,

$$\Delta(K) < V(K)/3.296\cdots.$$

In a paper, which is to appear in the Duke Math. Jour., Professor Davenport and I use a method similar to that of Dr. Mahler to obtain some further improvements).

UNIVERSITY COLLEGE,
UNIVERSITY OF LONDON

[10] H. MINKOWSKI, *Geometrie der Zahlen* (Leipzig, 1910), para. 51. H. DAVENPORT, *The product of n homogeneous linear forms*, Konik. Nederland. Akad. van Wetenshappen, **69** (1946), 822–828 (825) reproduces this proof; he also suggests as a problem the question whether or not the corresponding result is true for an arbitrary convex body.

[11] K. MAHLER, *On lattice points in star bodies*, Roy. Soc. London, Proc., A **187** (1946), 151–187 (Theorem 8).