AN ASYMPTOTIC EXPRESSION FOR THE NUMBER OF SOLUTIONS OF A GENERAL CLASS OF DIOPHANTINE EQUATIONS[1]

BY

GEORGE E. ANDREWS

Consider a closed, strictly convex body C defined by $f(x_1, \cdots, x_n) \leqq R$. If $f(x_1, \cdots, x_n)$ is a homogeneous function, it is easily verified that N, the number of solutions of $f(x_1, \cdots, x_n) = R$ in integers, satisfies the inequality $cR^{n-1} > N$. The object of this paper is to show that this inequality may be replaced by $cR^{(n-1)n/(n+1)} > N$. This result will be derived from the following theorem.

THEOREM. *We are given a closed, strictly convex body C with N lattice points (i.e. points with integer coordinates) on its surface. If $S(C)$ denotes the surface content of the boundary of C, then there exists a constant $k(n)$ depending only on n such that*

$$S(C) > k(n)N^{(n+1)/n},$$

where n denotes the dimensionality of space.

We shall now prove four lemmas and then prove this theorem.

LEMMA 1. *If*

$$\sum_1^a r_n(m) \leqq N < \sum_1^{a+1} r_n(m),$$

then

$$\sum_1^a m^{1/2} r_n(m) > c(n)N^{(n+1)/n}.$$

By $r_n(m)$, we mean the number of representations of m as the sum of n squares.

Proof. We have

$$\sum_1^M r_n(m) = \pi^{n/2}M^{n/2}/\Gamma(n/2 + 1) + O(M^{(n-1)/2})$$

[3, p. 271]. Hence it is clear that the a defined in the lemma is such that

$$a \sim c_1(n)N^{2/n}.$$

Thus

This paper has been submitted to and accepted for publication by the Proceedings of the American Mathematical Society. It has been transferred to these Transactions, with the consent of the author, for technical reasons. Received by the editors June 6, 1960.

(1) This paper is a condensation of the author's Master's thesis submitted at Oregon State College.

$$\sum_1^a m^{1/2} r_n(m) = a^{1/2} \sum_{m=1}^{a} r_n(m) - \sum_{m=1}^{a-1} \left\{ ((m+1)^{1/2} - m^{1/2}) \cdot \sum_{i=1}^{m} r_n(i) \right\}$$

$$= a^{1/2} \left[\frac{\pi^{n/2} a^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)} + O(a^{(n-1)/2}) \right]$$

$$- \sum_{m=1}^{a-1} \left(\frac{1}{2m^{1/2}} + O(m^{-3/2}) \right) \left[\frac{\pi^{n/2} m^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)} + O(m^{(n-1)/2}) \right]$$

$$= \frac{\pi^{n/2} a^{(n+1)/2}}{\Gamma\left(\frac{n}{2}+1\right)} + O(a^{n/2}) - \sum_1^{a-1} \left[\frac{\pi^{n/2} m^{(n-1)/2}}{2\Gamma\left(\frac{n}{2}+1\right)} + O(m^{(n-2)/2}) \right]$$

$$= \frac{\pi^{n/2} a^{(n+1)/2}}{\Gamma\left(\frac{n}{2}+1\right)} + O(a^{n/2}) - \frac{\pi^{n/2} (a-1)^{(n+1)/2}}{(n+1)\Gamma\left(\frac{n}{2}+1\right)} + O(a^{n/2})$$

$$= c_2(n) N^{(n+1)/n} + O(N).$$

Since $\sum_1^a m^{1/2} r_n(m)$ is a positive, increasing function of N, we have

$$\sum_1^a m^{1/2} r_n(m) > c(n) N^{(n+1)/n} \qquad \text{for all } N. \qquad \text{q.e.d.}$$

The following lemmas will concern a closed, strictly convex body C. We shall be given the fact that C contains N lattice points on its boundary. We shall call the set of boundary lattice points $B(N)$ and shall assume that not all members of $B(N)$ are linearly dependent. If all members of $B(N)$ were linearly dependent, we would only need to consider a space of lower dimensionality.

LEMMA 2. *The members of $B(N)$ are the vertices of a convex polytope entirely in the interior of C.*

Proof. Since a convex polytope is defined as the convex cover of a finite number of points, we see that the convex cover of $B(N)$ is a polytope entirely in the interior of C. Call this polytope $(Po)_n^a$. Clearly all vertices of $(Po)_n^a$ are members of $B(N)$ [2, pp. 24 and 29].

We need only show that all members of $B(N)$ are vertices of $(Po)_n^a$. Let $P \in B(N)$. Choose a regular supporting hyperplane S_{n-1} to C at P. Any two-dimensional segment s_1 which contains P either lies in S_{n-1} or it does not. If s_1 lies in S_{n-1}, then the only point of $(Po)_n^a$ contained by s_1 is P. Thus points of the exterior of $(Po)_n^a$ are contained by s_1. If s_1 doesn't lie on S_{n-1}, the part of s_1 lies on the opposite of S_{n-1} from $(Po)_n^a$. Thus, again, points of the exterior

of $(Po)_n^a$ are contained by s_1. Hence no segment completely on the boundary of $(Po)_n^a$ contains P. Thus P is a vertex of $(Po)_n^a$. q.e.d.

In the next lemma, we multiply each linear dimension of space by 3. In this way, $(Po)_n^a$ is transformed into a similar polytope $(Po)_n^b$. We shall denote the set of vertices of $(Po)_n^b$ by $B'(N)$. Since every vertex of $(Po)_n^b$ will be congruent with all the other members of $B'(N)$ modulo 3, the surface content of $(Po)_n^b$ will be 3^{n-1} times that of $(Po)_n^a$.

LEMMA 3. *It is possible to form from $(Po)_n^b$ a convex polytope, $(Po)_n^c$, in the interior of $(Po)_n^b$ with lattice point vertices and with at least N $(n-1)$-boundaries where N is the number of vertices of $(Po)_n^b$.*

Proof. In forming $(Po)_n^b$, we have multiplied every linear dimension of space by 3. Thus, each segment between two vertices of $(Po)_n^b$ will be divided into thirds by two lattice points. Let us form a set Σ consisting of these two lattices points taken from each segment between two vertices of $(Po)_n^b$. We define $(Po)_n^c$ as the convex cover of Σ. The polytope $(Po)_n^c$ is in the interior of $(Po)_n^b$ by construction. Clearly only members of Σ are vertices of $(Po)_n^c$ [2, pp. 24 and 29].

Pick a point X in the interior of $(Po)_n^c$. Clearly $(Po)_n^c$ has an interior for no edge of $(Po)_n^b$ is completely destroyed in the formation of $(Po)_n^c$, and not all members of $B'(N)$ are linearly dependent so that $(Po)_n^b$ has an interior.

We shall now show that any member of $B'(N)$ is in the exterior of $(Po)_n^c$. Let us choose a regular supporting hyperplane S'_{n-1} to $(Po)_n^b$ at any member of $B'(N)$, say P. We see that all members of Σ lie on one side of S'_{n-1} and none on S'_{n-1}. Therefore, P is neither in nor on the convex cover of Σ.

It follows from the above that the segment PX intersects the boundary of $(Po)_n^c$ in a single point for each $P \in B'(N)$.

Assume that $P \in B'(N)$ and $Q \in B'(N)$. We shall now show that the segments PX and QX do not intersect the same $(n-1)$-boundary of $(Po)_n^c$. Assume that PX and QX intersect the same $(n-1)$-boundary f'_{n-1} of $(Po)_n^c$. Let us consider the hyperplane S''_{n-1} containing f'_{n-1}. The segment PQ contains two members of Σ by definition. However, the convex cover of Σ is either on S''_{n-1} or on the opposite side of S''_{n-1} from P and Q, a contradiction. Hence to each segment PX for $P \in B'(N)$ corresponds a single $(n-1)$-boundary of $(Po)_n^c$.

Thus $(Po)_n^c$ satisfies all the conditions of the lemma. q.e.d.

LEMMA 4. *We are given an $(n-1)$-dimensional simplex with lattice point vertices. This simplex lies in the hyperplane S'''_{n-1} defined by*

$$A_1(x_1 - p_1) + A_2(x_2 - p_2) + \cdots + A_n(x_n - p_n) = 0$$

where all the A's are integers, $P(p_1, p_2, \cdots, p_n)$ is a vertex of the simplex, and g.c.d. $(A_1, A_2, \cdots, A_n) = 1$. Then the content of the above simplex is at least

$$\frac{1}{(n-1)!}(A_1^2 + A_2^2 + \cdots + A_n^2)^{1/2}.$$

Proof. Let us assume that P is the origin. If this is not so, we merely translate P into the origin. The equation of S'''_{n-1} is now

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = 0.$$

Since such a translation transforms lattice points into lattice points, we see that all the vertices of the considered simplex are still lattice points. Let us consider the $(n-1)$ edges of this simplex emanating from the origin as fixed position vectors of the form $(a_{i1}, a_{i2}, \cdots, a_{in})$. The end points of these vectors lie on the hyperplane

$$\begin{vmatrix} x_1 & x_2 & \cdots & x_n \\ a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{(n-1)1} & a_{(n-1)2} & & a_{(n-1)n} \end{vmatrix} = 0.$$

But this hyperplane is merely S'''_{n-1}. Hence the above determinant must expand into

$$k(A_1x_1 + A_2x_2 + \cdots + A_nx_n) = 0.$$

Since the components of all the vectors considered are integers and since g.c.d. $(A_1, A_2, \cdots, A_n) = 1$, we have $k \geqq 1$.

Let us consider the content of a parallelotope defined by the unit normal vector to S'''_{n-1} and the $(n-1)$ vectors of the form $(a_{i1}, a_{i2}, \cdots, a_{in})$. The content of this parallelotope will be numerically equal to the $(n-1)$-dimensional content of its base. Thus if $(b_1, b_2, \cdots, b_n)$ denotes the unit normal vector, we have

$$\frac{1}{(n-1)!}\begin{vmatrix} b_1 & b_2 & \cdots & b_n \\ a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{(n-1)1} & a_{(n-1)2} & & a_{(n-1)n} \end{vmatrix} = V_{n-1}$$

where V_{n-1} is the content of the simplex under consideration. However,

$$(b_1, b_2, \cdots, b_n) = (A_1^2 + A_2^2 + \cdots + A_n^2)^{-1/2}(A_1, A_2, \cdots, A_n).$$

Substituting this into the above determinant, we obtain

$$V_{n-1} = \frac{k(A_1^2 + A_2^2 + \cdots + A_n^2)}{(n-1)!(A_1^2 + A_2^2 + \cdots + A_n^2)^{1/2}}$$

$$\geqq \frac{1}{(n-1)!}(A_1^2 + A_2^2 + \cdots + A_n^2)^{1/2}. \qquad \text{q.e.d.}$$

We are now in a position to prove the main theorem. We shall restate it here for convenience.

THEOREM. *We are given a closed, strictly convex body C with N lattice points on its surface. If $S(C)$ denotes the surface content of the boundary of C, then there exists a constant $k(n)$ depending only on n such that*

$$S(C) > k(n)N^{(n+1)/n},$$

where n denotes the dimensionality of space.

NOTE. In this proof we shall use the fact that if one convex body is contained in another, then the first has smaller surface area (content) than the second [1, p. 47]. This follows from Cauchy's surface area formula.

We shall start the proof assuming that from C we have constructed $(Po)_n^a$, $(Po)_n^b$, and $(Po)_n^c$.

Proof. By Lemma 2, $(Po)_n^a$ is in the interior of C. Thus

$$S(C) \geqq S[(Po)_n^a].$$

From the remarks prefacing Lemma 3, we have

$$S[(Po)_n^a] \geqq 3^{-(n-1)}S[(Po)_n^b].$$

From Lemma 3, we have

$$S[(Po)_n^b] \geqq S[(Po)_n^c].$$

Hence

$$S(C) \geqq 3^{-(n-1)}S[(Po)_n^c].$$

Let us pick one $(n-1)$-dimensional simplex from each $(n-1)$-boundary of $(Po)_n^c$. By Lemma 3, $(Po)_n^c$ has at least N $(n-1)$-boundaries. Hence if $S(m)$ denotes the $(n-1)$-dimensional content of the mth simplex chosen, then

$$S[(Po)_n^c] \geqq \sum_{m=1}^{N} S(m).$$

However, no three $(n-1)$-boundaries of $(Po)_n^c$ may have the same direction numbers. If three $(n-1)$-boundaries of $(Po)_n^c$ had the same direction numbers, then two of these $(n-1)$-boundaries would be on opposite sides of the

hyperplane containing the third. By Lemma 4, we know that any simplex on a hyperplane of direction numbers $(A_1:A_2:\cdots:A_n)$ has content not less than

$$\frac{1}{(n-1)!}(A_1^2+A_2^2+\cdots+A_n^2).$$

Thus by Lemma 4, there will be no more than $r_n(1)$ simplexes among those chosen of content $1/(n-1)!$; there will be no more than $r_n(2)$ simplexes among those chosen of content $2/(n-1)!$, etc. Thus, if

$$\sum_{m=1}^{a} r_n(m) \leqq N < \sum_{m=1}^{a+1} r_n(m),$$

then

$$\sum_{m=1}^{N} S(m) \geqq \frac{1}{(n-1)!}\sum_{m=1}^{a} m^{1/2} r_n(m).$$

Hence by Lemma 1,

$$\sum_{m=1}^{N} S(m) \geqq \frac{c_2(n)}{(n-1)!} N^{(n+1)/n}.$$

Thus combining the above results, we obtain

$$S(C) \geqq k(n)N^{(n+1)/n}. \qquad \text{q.e.d.}$$

We may now easily verify the inequality stated at the beginning of this paper. Since $f(x_1, \cdots, x_n) = R$ is homogeneous we see that its surface content is given by $c''R^{n-1}$. Thus by the above theorem,

$$c''R^{n-1} > k(n)N^{(n+1)/n},$$

or

$$cR^{(n-1)n/(n+1)} > N.$$

Bibliography

1. T. Bonnesen and W. Fenchel, *Theorie der konvexen Körper*, New York, Chelsea, 1948, 164 pp.

2. H. G. Eggleston, *Convexity*, Cambridge, Cambridge University Press, 1958, Cambridge Tracts in Mathematics and Mathematical Physics, no. 47.

3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 3d ed., Oxford, Oxford University Press, 1954, 419 pp.

Oregon State College,
Corvallis, Oregon