RECENT PROGRESS IN THE GEOMETRY OF NUMBERS

H. DAVENPORT

In this address I shall endeavour to give an account of some of the work which has been done on the geometry of numbers since the time of the last Congress. At that Congress, Professor Mordell gave an address[1] on *Minkowski's theorems and hypotheses concerning linear forms*, in which he discussed two unproved conjectures of Minkowski; and it may be appropriate if I begin today by mentioning the progress that has since been made in connection with these two conjectures.

The first conjecture concerns what we should now call *the critical lattices of an n-dimensional cube*. A lattice in n dimensional space consists of all points $(x_1, \cdots, x_n)$ given by n linear forms in n variables $u_1, \cdots, u_n$ which take all integral values. In other words, a lattice is an affine transform of the set of all points with integral coordinates. Given a bounded region K in n-dimensional space, which contains the origin 0 as an inner point, we consider all those lattices which have no point except 0 in the interior of K. The lower bound of their determinants is called the *critical determinant* of K, denoted by $\Delta(K)$, and the lattices for which this lower bound is attained are called the *critical lattices* of K. In the case when K is the unit cube defined by

$$|x_1| \leqq 1, \cdots, |x_n| \leqq 1,$$

Minkowski proved that $\Delta(K) = 1$, and he made a conjecture about the nature of the critical lattices of K. The conjecture was that these lattices are given essentially by linear forms with triangular matrices and with unit elements in the principal diagonal.

There is an alternative way of formulating the conjecture, which is perhaps more readily grasped. A lattice is a critical lattice for the cube K if and only if it provides a space-filling for the cube $K/2$, so that when the cube $K/2$ is translated to have its centre at each lattice point, the resulting cubes exactly fill up space. The alternative form of the conjecture is that such a space-filling must necessarily be built up in layers, parallel to one of the coordinate planes. The cubes in any one layer constitute an $(n - 1)$-dimensional space-filling, and the successive layers are obtained by applying repeatedly a certain translation. In two or three dimensions, it is easy to see that this must be so, and proofs were given by Minkowski himself. The general conjecture, after resisting the efforts of all who had worked on it from the time of Minkowski, was eventually proved by Hajós in 1940.[2] His proof is based on an interpretation of the space-filling situation in terms of group-algebra.

[1] L. J. Mordell, Comptes Rendus du Congrès International des Mathématiciens, Oslo 1936, vol. 1, pp. 226–238.

[2] G. Hajós, Math. Zeit. vol. 47 (1941) pp. 427–467. Some simplifications in the proof have been made by L. Rédei, Acta Univ. Szeged. vol. 13 (1949) pp. 21–35, or Comment. Math. Helv. vol. 23 (1949) pp. 272–281, and T. Szele, Publicationes Math. (Debrecen) vol. 1 (1949) pp. 56–62.

The second of Minkowski's conjectures relates to quite a different question. Suppose we have any lattice of determinant 1 in n-dimensional space. The conjecture is that for any point $(c_1, \cdots, c_n)$ in the space there is a lattice point $(x_1, \cdots, x_n)$ such that

$$(1) \qquad |(x_1 - c_1) \cdots (x_n - c_n)| \leqq 1/2^n.$$

In other words, the product of n nonhomogeneous linear forms of determinant 1 always assumes a value $\leqq 1/2^n$, for integral values of the variables.

Minkowski himself proved this in the case $n = 2$, and many other proofs for that case are known. The case $n = 3$ was settled by Remak[3] in 1923, and the case $n = 4$ by Dyson[4] in 1946. In these cases, rather more is proved than is actually asserted in Minkowski's conjecture. What is proved is that it is possible to distort the lattice, by a transformation of the form

$$(2) \qquad y_1 = \lambda_1 x_1, \cdots, y_n = \lambda_n x_n \qquad (\lambda_1 \cdots \lambda_n = 1),$$

so that the new lattice in y space has its points distributed throughout the space with a certain uniformity. The precise meaning of this is that for any point $(d_1, \cdots, d_n)$ there is a lattice point $(y_1, \cdots, y_n)$ such that

$$(3) \qquad (y_1 - d_1)^2 + \cdots + (y_n - d_n)^2 \leqq \tfrac{1}{4}n.$$

Taking $d_1 = \lambda_1 c_1, \cdots, d_n = \lambda_n c_n$, it follows by the inequality of the arithmetic and geometric means that (1) holds. The method of choosing the multipliers $\lambda_1, \cdots, \lambda_n$ is to select them so that the quadratic form

$$(4) \qquad (\lambda_1 x_1)^2 + \cdots + (\lambda_n x_n)^2$$

attains its minimum value at n independent lattice points in x-space. In other words, the distorted lattice has n independent lattice points at the same minimal distance from the origin. Thus the proofs when $n = 3$ and $n = 4$ fall into two stages, the first stage being the proof that multipliers $\lambda_1, \cdots, \lambda_n$ with this property exist, the second stage being the proof that when they have been so chosen, the lattice in y-space has the property formulated in (3). Both stages become very difficult when $n = 4$, but more especially the first stage. Dyson establishes the existence of the λ's by topological arguments in the three-dimensional space of $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, treated as homogeneous coordinates. These arguments are subtle and novel, at least in this connection.

The question whether the situation in the n-dimensional space is similar, if one is content with less exact constants, was stressed by Mordell in his Oslo lecture, although he expressed it in a slightly different form. This question was answered affirmatively by Siegel[5] in 1937. He proved that it is possible to choose the multipliers $\lambda_1, \cdots, \lambda_n$ so that the successive minima of the quadratic form (4), though not necessarily equal, have their ratios bounded by constants

[3] R. Remak, Math. Zeit. vol. 17 (1923) pp. 1–34; vol. 18 (1923) pp. 173–200. A simpler proof was given by H. Davenport, J. London Math. Soc. vol. 14 (1939) pp. 47–51.

[4] F. J. Dyson, Ann. of Math. vol. 49 (1948) pp. 75–81, 82–109.

[5] See H. Davenport, Acta Arithmetica vol. 2 (1937) pp. 262–265.

depending only on n. If the λ's are chosen in this way, results analogous to (3) and (1) follow, but with large constants, depending on n, on the right-hand sides.

As early as 1934, Tschebotareff[6] had made an important contribution to Minkowski's problem, using quite a different method. His work, however, did not receive adequate publicity until several years later. What he proved was that Minkowski's conjecture, expressed by (1), is true if instead of $1/2^n$ on the right, there stands any number greater than $1/(2^{1/2})^n$. The proof is simple and ingenious, though it does not establish the possibility of distorting the lattice so that it has a property analogous to that expressed by (3). The method underlying Tschebotareff's work has recently been generalized by Macbeath,[7] and expressed by him in the form of a general principle, applicable to a variety of problems.

In spite of all the work I have mentioned, Minkowski's conjecture remains unproved, and is an outstanding challenge to all who are interested in the subject.

There are particular cases which invite detailed study. The case when the linear forms $x_1, \cdots, x_n$ have rational coefficients is almost trivial, since then one can transform them into diagonal form, and satisfy (1) by choosing the integral variables $u_1, \cdots, u_n$ one at a time. A case which gives rise to interesting considerations is that in which the linear forms $x_1, \cdots, x_n$ correspond to a totally real algebraic number-field of degree n. We take x_1 to be the linear form which represents the general algebraic integer of the field, and $x_2, \cdots, x_n$ to be the algebraically conjugate linear forms. The problem then is: how small can one make $|(x_1 - c_1) \cdots (x_n - c_n)|$ for arbitrary real numbers $c_1, \cdots, c_n$? Allowing for the fact that the determinant of the linear forms is no longer 1 but $d^{1/2}$, where d is the discriminant of the field, Minkowski's conjecture (known to be true for $n \leqq 4$) would imply that we can make the product less than $2^{-n}d^{1/2}$. For any particular number-field F there will be a best possible estimate $\mathfrak{M}(F)$ for the product, and this constant has been determined for several quadratic and cubic fields.[8] The problem is one which, if appropriately formulated, retains its significance when F is not totally real, although Minkowski's conjecture is no longer relevant and $\mathfrak{M}(F)$ is no longer of the order $d^{1/2}$.

The problem just mentioned (that of determining, or estimating, the number $\mathfrak{M}(F)$) has a bearing on the question of the validity or invalidity of Euclid's algorithm in the field F. If $\mathfrak{M}(F) > 1$ for a particular field F, then there exist

[6] N. Tschebotareff, Scientific Notes of Kazan University vol. 94 Part 7 (1934) pp. 4–16; also in Vierteljahresschrift der Naturforschenden Gesellschaft in Zürich vol. 85 (1940) pp. 27–30. The proof is also accessible in Hardy and Wright, *Introduction to the theory of numbers*, 2d ed., 1945, p. 396.

[7] A. M. Macbeath, in his Princeton Ph.D. dissertation, not yet published.

[8] The literature for quadratic fields is somewhat extensive. For cubic fields, see H. Davenport, Proc. Cambridge Philos. Soc. vol. 43 (1947) pp. 137–152; A. V. Prasad, Neder. Akad. Wetensch. vol. 52 (1949) pp. 240–250, 338–350; L. E. Clarke, Quart. J. Math. Oxford Ser. (in course of publication).

numbers $c_1, \cdots, c_n$ (all real if F is totally real, and otherwise real or complex in correspondence with F and its conjugate fields) such that

$$| (x_1 - c_1) \cdots (x_n - c_n) | > 1$$

for all integers x_1 of F. If these numbers can be so chosen that c_1 is a nonintegral number of F, and $c_2, \cdots, c_n$ are the algebraic conjugates of c_1, the product becomes the norm of $x_1 - c_1$, and it follows that Euclid's algorithm does not hold in the field F. For real quadratic fields, I proved[9] in 1948 that

$$\mathfrak{M}(F) > \frac{1}{128} d^{1/2},$$

and further that this remains true if c_1, c_2 are restricted in the way described above. It follows that Euclid's algorithm cannot hold in a real quadratic field if $d > (128)^2$. This result led to the final enumeration[10] of all the real quadratic fields in which the algorithm holds. I have since proved a similar inequality for $\mathfrak{M}(F)$ for two other types of field, namely (a) cubic fields of negative discriminant, and (b) totally complex quartic fields; and have proved in this way that there are only a finite number of such fields for which Euclid's algorithm holds.[11]

We now turn from Minkowski's two conjectures, and questions connected with them, to the geometry of numbers as a whole. There have been so many developments in the subject in the last fourteen years that we can only mention briefly a selection of them. The central problem of the subject is that of finding the critical determinant $\Delta(K)$ of a given region K, which we suppose for the present to be bounded. It is convenient to consider the ratio $\Delta(K)/V(K)$, where $V(K)$ is the volume of K, since the ratio is invariant under affine transformations. Two general theorems concerning this ratio are known. The first is the fundamental theorem of Minkowski, which states that

$$\frac{\Delta(K)}{V(K)} \geqq \frac{1}{2^n}$$

provided K is convex and symmetrical about 0. The reason for the theorem lies in the equivalence (for convex bodies) between the problem of the critical determinant and the problem of closest packing; and the inequality simply expresses the fact that the density of closest packing cannot exceed 1.

The second theorem is an inequality in the opposite direction, which was

[9] H. Davenport, Proc. London Math. Soc. (in course of publication). See also H. Davenport, Quart. J. Math. Oxford Ser. (2) vol. 1 (1950) pp. 54–62.

[10] See H. Chatland and H. Davenport, Canadian Journal of Mathematics vol. 2 (1950) pp. 289–296, and K. Inkeri, Annales Academiae Scientiarum Fennicae. Ser. A vol. 41 (1948) pp. 5–34.

[11] H. Davenport, Acta Math. vol. 84 (1950) pp. 159–179 and Trans. Amer. Math. Soc. vol. 68 (1950) pp. 508–532.

stated by Minkowski in his last paper on the geometry of numbers, but without proof. It is that

$$\frac{\Delta(K)}{V(K)} \leqq \frac{1}{2\zeta(n)},$$

where $\zeta(n) = 1 + 2^{-n} + 3^{-n} + \cdots$, provided that K is a symmetrical star body relative to 0. The first general proof was given by Hlawka[12] in 1943, and simpler proofs were given later, first by Siegel[13] and then by Rogers.[14] The result is essentially an existence theorem: it asserts, in effect, the existence of a lattice having no point except 0 in K, and having a determinant which is bounded in terms of $V(K)$. All the proofs depend on "averaging" arguments, applied to lattices of a given determinant.

We have, then, these two general estimates for $\Delta(K)/V(K)$. Each of them can be improved by imposing further restrictions on K. In the case of an n-dimensional sphere, the lower estimate was greatly improved by Blichfeldt in two famous papers,[15] but even in this case there is a wide gap between the best known estimates from above and from below.

Minkowski developed a systematic procedure for determining $\Delta(K)$ when K is a two-dimensional or three-dimensional region which is convex and symmetrical about 0. Mahler[16] has adapted this procedure so that it applies to bounded star regions in the plane, not necessarily convex, and detailed results have been worked out by him and by his pupils for many particular regions, both convex and nonconvex.

Let us now turn to unbounded regions, which are in various ways more interesting than bounded regions. All the regions we shall consider will be star bodies relative to 0 and symmetrical about 0. We again define the critical determinant of a region K to be the lower bound of the determinants of all lattices which have no point except 0 in the interior of K. It may be, however, that *every* lattice has a point other than 0 in the interior of K; in this case we make the natural convention that $\Delta(K) = \infty$. One of the most interesting problems of the subject is to find criteria which will decide whether $\Delta(K)$ is finite or infinite. One obvious fact is that $\Delta(K)$ will be infinite if K contains convex regions, symmetrical about 0, of arbitrarily large volume, but this does not say much.

There are a few unbounded regions for which $\Delta(K)$ is known already from classical results concerning the corresponding Diophantine inequalities. These are the regions which correspond to indefinite quadratic forms in two, three, or

[12] E. Hlawka, Math. Zeit. vol. 49 (1943) pp. 285–312.

[13] C. L. Siegel, Ann. of Math. vol. 46 (1945) pp. 340–347.

[14] C. A. Rogers, Ann. of Math. vol. 48 (1947) pp. 996–1002.

[15] H. F. Blichfeldt, Trans. Amer. Math. Soc. vol. 15 (1914) pp. 227–235, and Math. Ann. vol. 101 (1929) pp. 605–608.

[16] K. Mahler, J. London Math. Soc. vol. 17 (1942) pp. 130–133, and other papers.

four variables; namely

$$| xy | \leqq 1 \qquad \text{in two dimensions,}$$

$$| x^2 + y^2 - z^2 | \leqq 1 \qquad \text{in three dimensions,}$$

$$\left.\begin{array}{r} | x^2 + y^2 + z^2 - w^2 | \leqq 1 \\ | x^2 + y^2 - z^2 - w^2 | \leqq 1 \end{array}\right\} \text{in four dimensions.}$$

The critical determinants of all these regions follow at once from classical work of Korkine and Zolotareff, and Markoff, on the minima of indefinite quadratic forms.[17] When we come to the corresponding regions in five or more dimensions, we meet precisely the problem mentioned above. It is conjectured that *every* lattice, no matter how large its determinant may be, has a point other than 0 in the n-dimensional region

$$| \pm x_1^2 \pm x_2^2 \pm \cdots \pm x_n^2 | \leqq 1,$$

where the signs are fixed but not all the same, and $n \geqq 5$. In the cases $n \leqq 4$, the critical lattices of the regions are lattices for which the corresponding quadratic form (xy or $x^2 + y^2 - z^2$, etc.) becomes a certain special quadratic form with integral coefficients in the u variables, namely the form of least determinant which does not represent zero. Now there is a theorem of Meyer which states that any indefinite form with integral coefficients in five or more variables necessarily represents zero, and this is the main ground for conjecturing that the critical determinant of the n-dimensional region is infinite when $n \geqq 5$. Expressed arithmetically, the conjecture is that any indefinite quadratic form in five of more variables assumes values which are arbitrarily small numerically, for integral values of the variables, not all zero. This conjecture presents one of the most interesting unsolved problems in the subject.

In 1937 I found the critical determinant of another unbounded region, namely the three-dimensional region defined by $| xyz | \leqq 1$; and this proved to be the starting point for a good deal of new work. The value of the critical determinant is 7, and the critical lattices are closely related (as indeed was expected) to a particular cubic field. This is the cubic field of least positive discriminant, 49, and is generated by the equation $\theta^3 + \theta^2 - 2\theta - 1 = 0$. If ξ is the linear form which represents the general algebraic integer of this field, the critical lattices for the region in question are given by

$$x = \lambda\xi, \qquad y = \mu\xi', \qquad z = \nu\xi'',$$

where accents denote algebraic conjugates, and λ, μ, ν are any constants with $\lambda\mu\nu = \pm 1$. The linear forms x, y, z have determinant 7, and xyz is a nonzero

[17] For the results concerning quadratic forms, see P. Bachmann, *Die Arithmetik der quadratischen Formen* II, and L. E. Dickson, *Studies in the theory of numbers*. For a simple proof of Markoff's results on binary forms, see J. W. S. Cassels, Ann. of Math. vol. 50 (1949) pp. 676–685. New results on ternary forms have been given by A. Venkov, Bull. Acad. Sci. URSS. Sér. Math. vol. 9 no. 6 (1945).

integer for all values of the integral variables, not all zero. My original proof[18] of these results was complicated, but later I found a much simpler proof[19] on the same general lines.

In 1938 I found the critical determinant of the three-dimensional region defined by

$$| x(y^2 + z^2) | \leqq 1,$$

its value being $(23)^{1/2}/2$. The proof[20] was complicated, and even now no simple direct proof is known. The critical lattices are related in a similar way to a particular cubic field, namely the field of numerically least negative discriminant, -23. This last fact is rather difficult to prove, and has only recently been established[21] by using methods due to Mahler.

The corresponding problems in four dimensions are still unsolved.

In 1940, Mordell found a new method of approach to the three-dimensional regions just discussed. He showed[22] that the results could be deduced from similar results for certain two-dimensional regions. The two-dimensional region required for $| xyz | \leqq 1$ was that given by

$$| xy(x + y) | \leqq 1,$$

which has the critical determinant $7^{1/3}$. That required for $| x(y^2 + z^2) | \leqq 1$ was given by

$$| x(x^2 + y^2) | \leqq 1,$$

which has the critical determinant $((23)^{1/2}/2)^{1/3}$. Two-dimensional regions are naturally easier to deal with than three-dimensional regions, although in the present case the gain in simplicity is partially compensated for by the fact that the two-dimensional regions do not possess the continuous infinity of automorphisms which is the main feature of the three-dimensional regions.

Mordell gave several proofs[23] of his two-dimensional results, and the methods which he evolved for the purpose proved to be applicable to other regions in the plane, some of them being regions of a certain degree of generality. It is a striking fact that it is often easier to find the critical determinant of a nonconvex region than of a convex region whose definition is superficially similar. For example, Mordell found the critical determinant of the nonconvex region $| x |^p + | y |^p \leqq 1$

[18] H. Davenport, Proc. London Math. Soc. (2) vol. 44 (1938) pp. 412–431.

[19] H. Davenport, J. London Math. Soc. vol. 16 (1941) pp. 98–101. See also Proc. Cambridge Philos. Soc. vol. 39 (1943) pp. 1–21.

[20] H. Davenport, Proc. London Math. Soc. (2) vol. 45 (1939) pp. 98–125.

[21] See H. Davenport and C. A. Rogers, Phil. Trans. Roy. Soc. London Ser. A vol. 242 (1950) pp. 311–344.

[22] L. J. Mordell, J. London Math. Soc. vol. 16 (1941) pp. 83–85; vol. 17 (1942) pp. 107–115.

[23] L. J. Mordell, Proc. London Math. Soc. (2) vol. 48 (1943) pp. 198–228, 339–390; J. London Math. Soc. vol. 18 (1943) pp. 201–217, vol. 19 (1944) pp. 92–99.

for $0.33 < p < 1$, whereas our knowledge about the convex region defined by the same inequality when $p > 1$ is still only fragmentary. The explanation seems to be that the critical lattices of a nonconvex region often bear a simple relation to the shape of the region.

In 1946, Mahler[24] developed a general theory of star bodies in n-dimensional space, in which he clarified much that was previously obscure, and proved many general theorems, some of a positive and some of a negative character. He also introduced much of the terminology which we have been using throughout the discussion. One of his basic results is that if $\Delta(K)$ is finite, then certainly there exists at least one critical lattice for K. A critical lattice need not have any point on the boundary of K, but must of course have a point in the region $(1 + \epsilon)K$ for any $\epsilon > 0$. Mahler also proved that each of the special unbounded bodies we have mentioned (arising from quadratic forms or from products of coordinates) is *boundedly reducible*, that is, contains a bounded star body with the same critical determinant. Thus, for example, the body defined by

$$| xyz | \leqq 1, \qquad x^2 + y^2 + z^2 \leqq R^2$$

has the critical determinant 7, if R is sufficiently large. The proofs that these various special bodies are boundedly reducible all depend, however, on information already available about the critical determinant and critical lattices of the body. A general method for proving that a body is boundedly reducible would be of great interest. Mahler proposes many problems in his paper, and although some of these have since been solved, an ample number remain for the attention of future investigators.

The work of Mahler has been carried further in some directions by Rogers and myself.[25] We proved, for various unbounded star bodies, that any lattice of determinant less than $\Delta(K)$ must have not only one point but an infinity of points in the interior of K. We have also[26] drawn attention to some facts which are implicit in Mahler's work, concerning bodies such as $| xyz | \leqq 1$. Instead of reducing this to a bounded body, there are other ways in which it can be modified without changing the value of the critical determinant: for example, the region defined by

$$| x | (| x | + | y |) (| x | + | y | + | z |) \leqq 1$$

has the same critical determinant, namely 7, and the same critical lattices as the region defined by $| xyz | \leqq 1$. Mahler had already shown[24] that this was true for the region defined by

$$x^2y^2(x^2 + y^2 + z^2) \leqq 1,$$

[24] K. Mahler, Proc. Roy. Soc. London. Ser. A vol. 187 (1946) pp. 151–187; and Neder. Akad. Wetensch. vol. 49 (1946) pp. 331–343, 444–454, 524–532, 622–631.

[25] H. Davenport and C. A. Rogers, Phil. Trans. Roy. Soc. London. Ser. A vol. 242 (1950) pp. 311–344.

[26] H. Davenport and C. A. Rogers, J. London Math. Soc. vol. 24 (1949) pp. 271–280.

and had given this as a simple example of a region whose critical lattices have no points on the boundary. The basic reason for the validity of these results, which seem at first sight curious, lies in the simple form of the automorphisms of the region $|xyz| \leqq 1$:

$$x = \lambda x', \qquad y = \mu y', \qquad z = \nu z' \qquad\qquad (\lambda\mu\nu = \pm 1).$$

University College, University of London,
London, England.