A NEW PRINCIPLE IN THE GEOMETRY OF NUMBERS, WITH SOME APPLICATIONS

BY

H. F. BLICHFELDT

1. Minkowski has discovered a geometrical principle which he applied with success to certain important problems in the theory of numbers. If we define *lattice-points* as those points in space of n dimensions whose (rectangular) coördinates are positive or negative integers or zero, his principle may be stated as follows:*

A surface in n-dimensional space, nowhere concave, possessing a center which coincides with one of the lattice-points of this n-space, and having a volume $\geqq 2^n$, will contain at least two more lattice-points, either inside the surface or upon its boundary.

He gave this theorem the following analytic form: Let $f(x_1, \cdots, x_n)$ be any function of $x_1, \cdots, x_n$, which vanishes when $x_1 = 0, \cdots, x_n = 0$, but possesses a definite positive value for any other system of values assigned to $x_1, \cdots, x_n$; let, moreover, the following functional equations be fulfilled:

$$\text{(I)} \qquad f(tx_1, \cdots, tx_n) = tf(x_1, \cdots, x_n), \quad \text{when} \quad t > 0,$$

$$\text{(II)} \qquad f(y_1 + z_1, \cdots, y_n + z_n) \leqq f(y_1, \cdots, y_n) + f(z_1, \cdots, z_n),$$

$$\text{(III)} \qquad f(-x_1, \cdots, -x_n) = f(x_1, \cdots, x_n).$$

Then the n-tuple integral $\int dx_1 \cdots dx_n$, taken over the region

$$f(x_1, \cdots, x_n) \leqq 1$$

in positive directions along the paths of integration, will possess a definite value J, and there exists at least one system of integers $l_1, \cdots, l_n$, such that

$$0 < f(l_1, \cdots, l_n) \leqq \frac{2}{\sqrt[n]{J}}.$$

2. Among the applications given by Minkowski, two will be mentioned here, and one later on (§ 12).

* *Geometrie der Zahlen*, Leipzig und Berlin, 1910, p. 76.

(α) Let

$$[f(x_1, \cdots, x_n)]^2 \equiv \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

be a positive, definite quadratic form in n variables, having a determinant D. Then the variables may be replaced by such integers $l_1, \cdots, l_n$ that we have*

$$0 < f^2 \leqq \frac{4}{\pi}\left[\Gamma\left(1+\frac{n}{2}\right)\right]^{2/n} D^{1/n}.$$

(β) Let

$$f(x_1, \cdots, x_n) \equiv |v_1| + \cdots + |v_n|,$$

where $v_1, \cdots, v_n$ are linear homogeneous forms in $x_1, \cdots, x_n$, with a non-vanishing determinant Δ. Let s pairs of these forms have conjugate imaginary coefficients. Then integers $l_1, \cdots, l_n$ exist such that we have, upon substitution,*

$$0 < f \leqq \left[\left(\frac{4}{\pi}\right)^s \Gamma(1+n) \cdot |\Delta|\right]^{1/n}.$$

3. A new geometrical principle will now be stated and proved. To make it somewhat more general in scope, a new definition of lattice-points will be necessary.

DEFINITION. Let the n-space defined by rectangular coördinates $x_1, \cdots, x_n$ be divided into equal rectangular spaces by the n systems of planes

$$x_1 = a_1 + b_1 t, \cdots, x_n = a_n + b_n t \quad (t = 0, \pm 1, \pm 2, \cdots),$$

where $a_1, \cdots, a_n, b_1, \cdots, b_n$ are given real numbers. We shall call these spaces *fundamental parallelepipeds*. In each of them let there be located, in an arbitrary manner, a given number of points, say k; none of them, however, lying upon the boundaries of the parallelepipeds. *These points shall be designated lattice-points.*

It will be observed that this definition of lattice-points includes the former: set $a_i = \frac{1}{2}$, $b_i = 1$ $(i = 1, \cdots, n)$; and locate one lattice-point $(k = 1)$ at the center of each of the resulting parallelepipeds.

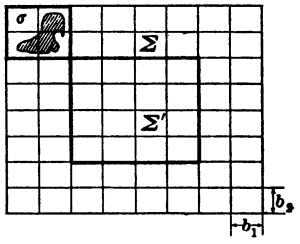
4. **Theorem I.** *Let S represent any limited open n-dimensional continuum in the n-space $x_1, \cdots, x_n$, having the (outer) volume V. By a suitable translation*

$$x_i' = x_i + \delta_i \qquad (i = 1, \cdots, n),$$

this continuum can be placed in such a position with reference to the fundamental parallelepipeds that the number of lattice-points L contained in the continuum or lying as near as we please to its boundary is greater than Vk/W, where W represents the volume, and k the number of lattice-points of a fundamental parallelepiped.

* *Geometrie der Zahlen*, p. 122.

Proof. We construct a parallelepiped σ whose edges parallel to the coördinate axes $X_1, \cdots, X_n$ are of lengths $Ab_1, \cdots, Ab_n$, A being a fixed integer (2 in the figure) taken so large that S can, by a translation, be placed entirely within σ. When so placed, the double surface obtained will be denoted by (S, σ). We then construct a parallelepiped Σ whose edges, parallel to the axes, are of lengths $Bb_1, \cdots, Bb_n$, B being a large (variable) integer (8 in the figure), which exceeds $2A$. We may assume that Σ contains just B^n fundamental parallelepipeds. Inside Σ we have a parallelepiped Σ' whose edges are of lengths $(B-2A)\,b_1, \cdots, (B-2A)\,b_n$, its faces being at distances $Ab_1, \cdots, Ab_n$ from those of Σ.



Now place (S, σ) in such a position inside Σ that one of the vertices of σ coincides with one of Σ, so that n of its faces lie upon n of the faces of Σ. From this position we obtain $\{(B-A)\,C+1\}^n$ different positions of (S, σ), all inside Σ, by means of translations of the form

$$x_i' = x_i + t_i \frac{b_i}{C} \qquad (i = 1, \cdots, n), \tag{1}$$

where t_i runs through all integral values from $-\infty$ to $+\infty$, independently for each subscript i, and where C represents a large positive integer.

5. Each of the $k\,(B-2A)^n$ lattice-points inside Σ' will lie inside or near to several of the surfaces S, if C be chosen large enough. We shall proceed to count these lattice-points in such a way that each is counted as often as it appears inside of, or as near as we please to a surface S. Call this number N.

Consider any one of these lattice-points P. To count the number of surfaces S inside of which it will appear, we may regard S as stationary and P as subjected to the translations (1). Then P will appear as vertices of parallelepipeds whose edges are of lengths $b_1/C, \cdots, b_n/C$. Let the least number of such parallelepipeds which entirely contain the continuum S be M_P. We may take C so large that all the vertices of these M_P parallelepipeds lie either within the continuum S, or as near as we please to its boundary. Summing for all of the lattice-points considered, we get

$$N > k\,(B-2A)^n\,M,$$

M being the smallest of the numbers M_P.

6. Since there are $\{(B-A)\,C+1\}^n$ different surfaces S inside Σ, it follows that there are

$$L > k\frac{(B-2A)^n\,M}{\{(B-A)\,C+1\}^n}$$

lattice-points inside or near the surface of at least one of them. If now B and C increase indefinitely, the right-hand member approaches

$$\lim_{C=\infty} k\frac{M}{C^n} = k\frac{V}{b_1 \cdots b_n} = \frac{k}{W}V$$

so that for a given positive ϵ we may take

$$L > \frac{k}{W}V - \epsilon.$$

Finally, since L is an integer, the inequality of the theorem follows unless Vk/W is an integer also. In this case however we consider first a continuum lying arbitrarily near to S and containing S within it. For this continuum of volume greater than V the desired inequality holds, and thus for S also. The theorem is therefore true.

7. When the different fundamental parallelepipeds are congruent with reference to the lattice-points contained, the statement in Theorem I reading "the number of lattice-points L contained in the continuum or lying as near as we please to limiting points of the continuum is greater than kV/W . . ." may be accentuated to read as follows: "*the number of lattice-points L contained in the continuum or belonging to limiting points of the continuum is greater than* Vk/W. . . ." The above proof may be modified to cover this statement. However, instead of doing this, we shall give a very elegant and independent proof of Theorem I, under the restrictions mentioned, furnished the author by Professor Birkhoff, which proof throws into evidence the sharper wording of the theorem. We shall limit ourselves to one lattice-point in each fundamental parallelepiped, although the proof, as given by Professor Birkhoff, is valid for any number. The spirit of the proof is shown equally well by limiting ourselves to space of two dimensions only.

Let us therefore assume the plane divided into a network R of equal rectangles, a single lattice-point A in each, similarly placed. Let a closed curve C be drawn, having an (outer) area V, the area of a rectangle being W.

We will superpose, by a translation, upon a single rectangle R_1 all those which are covered, in whole or in part, by V (its boundary included). It is then evident that a point P can be located in R_1 at which the superposed or adjoining portions of V are in number $L > V/W$, unless V/W = an integer and no part of the boundary of V appears inside R_1. But such a case could be avoided by subjecting C to a proper translation at the outset. In the reconstructed area V, P will appear as L points, congruent with reference to the rectangles R. Applying a translation such that these points coincide with L points A, the translated area V will contain in its interior or upon its boundary more than V/W lattice-points A.

8. **Extension of Theorem I.** *Let there be given a finite number of continua* $S_1, \cdots, S_m$, *overlapping or not, forming a network* $\bar{S}$, *and let* $\alpha_1, \cdots, \alpha_m$ *be arbitrary positive constants. Then by a suitable translation,* $\bar{S}$ *may be brought into such a position that, if* L_i *designates the number of lattice-points inside of or as near as we please to the surface of* S_i, *and* V_i *the outer volume of* S_i, *then* $\alpha_1 L_1 + \cdots + \alpha_m L_m > (\alpha_1 V_1 + \cdots + \alpha_m V_m)\, k / W$. The demonstration follows that of Theorem I, after S in the symbol (S, σ) is replaced by $\bar{S}$. Considering each continuum S_i in turn, we prove (using corresponding notation N_i, M_i):

$$\Sigma\alpha_i N_i > k\,(B - 2A)^n\, \Sigma\alpha_i M_i,$$

and then divide by $\{(B - 2A)\,C + 1\}^n$. Finally, $\Sigma\alpha_i L_i$ not being a continuous magnitude, the argument at the end of § 6 is valid here.

9. Minkowski's general analytical theorem (§ 1), so far as the last inequalities are concerned, follows immediately from Theorem I. Let the symbols $f(x_1, \cdots, x_n)$, J be defined as in Minkowski's theorem, and let S represent the continuum of points $(x_1, \cdots, x_n)$ satisfying the condition

$$f(x_1, \cdots x_n) < J^{-1/n}. \tag{2}$$

Then $V = 1$, and if "lattice-points" are defined as in § 1, we have $k/W = 1$ (cf. § 3). Applying Theorem I, we have $L \geqq 2$. Let $(y_1, \cdots, y_n)$ and $(-z_1, \cdots, -z_n)$ be two lattice-points inside S or upon its boundary (§ 7), in its new position. Set $y_1 + z_1 = l_1, \cdots, y_n + z_n = l_n$.

Now, if $(x_1', \cdots, x_n')$ be a lattice-point which after a translation lies in or on the boundary of the continuum defined by (2) and if $\delta_1, \cdots, \delta_n$ be the components of the translation, we have

$$f(x_1' - \delta_1, \cdots, x_n' - \delta_n) \leqq \frac{1}{J^{1/n}}.$$

Hence, we obtain

$$0 < f(l_1, \cdots, l_n) = f(y_1 + z_1, \cdots, y_n + z_n)$$
$$\leqq f(y_1 - \delta_1, \cdots, y_n - \delta_n) + f(-z_1 - \delta_1, \cdots, -z_n - \delta_n) \leqq 2J^{-1/n}.$$

10. **Quadratic forms.** Let F designate a positive definite quadratic form in n variables $x_1, \cdots, x_n$. We may write

$$F \equiv v_1^2 + \cdots + v_n^2,$$

where $v_1, \cdots, v_n$ are linear in the n variables and of determinant Δ. Then the determinant of F will be $D = \Delta^2$.

To apply the theorem in § 8, let us construct the network $\bar{S}$, consisting of the points respectively inside the surfaces $S_1, \cdots, S_m$; S_λ having for its

equation

$$F = (\lambda\phi)^{2/n}, \quad \text{where} \quad \phi = \frac{n+2}{2mJ};$$

here m is a large (variable) integer, and

$$J = \frac{\pi^{\frac{1}{2}n}}{\Delta\Gamma(1+\frac{1}{2}n)}$$

is the volume of $F = 1$. Let "lattice-points" be those points having integral coördinates, so that $k / W = 1$. Then, after a suitable translation,

$$\alpha_1 L_1 + \cdots + \alpha_m L_m > \alpha_1 V_1 + \cdots + \alpha_m V_m = \phi J(\alpha_1 + 2\alpha_2 + \cdots + m\alpha_m). \tag{3}$$

We shall put $\alpha_i = (i+1)^{2/n} - i^{2/n}$ when $i < m$,

$$\alpha_m = \frac{(n+2)g}{n\,m} - m^{2/n},$$

where $g = 1 + 2^{2/n} + \cdots + m^{2/n}$, and shall denote $L_i - L_{i-1}$ by p_i. Then (3) becomes

$$\frac{(n+2)g}{n\,m} L_m - (p_1 + 2^{2/n} p_2 + \cdots + m^{2/n} p_m) > \frac{(n+2)g}{n\,m}. \tag{4}$$

Now, if $x_1', \cdots, x_m'$ be a lattice-point inside or near S_λ, and if we indicate the result of substituting $x_1' - \delta_1, \cdots, x_n' - \delta_n$ for $x_1, \cdots, x_n$ in v_i by v_i', then

$$(v_1')^2 + \cdots + (v_n')^2 < (\lambda\phi)^{2/n} + \epsilon,$$

where ϵ is a quantity small at will. If $x_1'', \cdots, x_n''$ be any other lattice-point, then the differences $v_1' - v_1''$, etc., are equal to the results obtained by substituting the integers $x_1' - x_1''$, etc., for x_1, etc., in $v_1, \cdots, v_n$. Hence

$$(v_1' - v_1'')^2 + \cdots + (v_n' - v_n'')^2 \tag{5}$$

will be a numerical value of F, for integral values of the variables involved.

Adding all the expressions (5) for every pair of lattice-points contained in the network $\overline{S}$, and denoting the sum $p_1 + p_2 + \cdots + p_m = L_m$ by P, we get

$$P\sum_{j=1}^{P}\{(v_1^{(j)})^2 + \cdots + (v_n^{(j)})^2\} - \left(\sum_{j=1}^{P} v_1^{(j)}\right)^2 - \cdots - \left(\sum_{j=1}^{P} v_n^{(j)}\right)^2$$

$$< P\{p_1\phi^{2/n} + p_2(2\phi)^{2/n} + \cdots + p_m(m\phi)^{2/n}\} + \epsilon P^2$$

$$< P\phi^{2/n}(P-1)\frac{(n+2)g}{n\,m} + \epsilon P^2,$$

by (4). If we now divide by $\frac{1}{2}P(P-1)$, substitute the value of ϕ and pass to the limit $m = \infty$, we obtain

THEOREM II. *Let F be a positive definite quadratic form in n variables and of determinant D. Then integers $l_1, \cdots, l_n$, not all zero, may be substituted for the n variables such that the numerical value of F is not greater than*

$$\frac{2}{\pi}\left[\Gamma\left(1+\frac{n+2}{2}\right)\right]^{2/n} D^{1/n}$$

It will be observed that the asymptotic value $nD^{1/n}/\pi e$ of this expression is one half that of Minkowski's limit (§ 2). Minkowski* has proved that the asymptotic value cannot fall below $nD^{1/n}/2\pi e$. The actual limit for $n = 2$ was first determined by Hermite,† and for $n = 3$, 4 and 5 by Korkine and Zolotareff.‡ The quotients of these limits divided by $D^{1/n}$ are respectively $2/\sqrt{3}, \sqrt[3]{2}, \sqrt{2}, \sqrt[5]{8}$.

11. **Linear forms.** Let $f \equiv |v_1| + \cdots + |v_n|$, where $v_1, \cdots, v_n$ are linear homogeneous forms in $x_1, \cdots, x_n$, of determinant $\Delta \neq 0$. If imaginary coefficients occur we assume that the forms having such coefficients appear in conjugate imaginary pairs. We can then utilize Theorem II. For, from the value of $|v_1|^2 + |v_2|^2$, the maximum value of $|v_1| + |v_2|$ is obtained by putting $|v_1| = |v_2|$. We find the following

THEOREM III. *Integers $l_1, \cdots, l_n$, not all zero, can be substituted for the variables $x_1, \cdots, x_n$ such that*

$$0 < |v_1| + \cdots + |v_n| \leqq \sqrt{\frac{2n}{\pi}}\left[\Gamma\left(1+\frac{n+2}{2}\right)\right]^{1/n} |\Delta|^{1/n}.$$

The asymptotic value

$$\frac{n}{\sqrt{\pi e}}|\Delta|^{1/n}$$

of this limit is smaller than that (§ 2) of Minkowski

$$\frac{n}{e}\left(\frac{4}{\pi}\right)^{s/n}|\Delta|^{1/n},$$

the more so the greater the number of pairs s of conjugate imaginary forms contained among $v_1, \cdots, v_n$. On the other hand, for low values of n, the limit given above is higher than that given by Minkowski.

*Journal für Mathematik, vol. 129 (1905), pp. 268–9.

†Journal für Mathematik, vol. 40 (1850), p. 263. The limits for $n = 2$ and $n = 3$ were virtually determined by Gauss and Seeber. Cf. Gauss' Werke, Bd. 1, p. 307, ff. and Bd. 2, p. 192, ff. Göttingen, 1876.

‡*Sur les formes quadratiques positives*, Mathematische Annalen, vol. 11 (1877), p. 242, ff.

12. **Approximation of irrational numbers by means of fractions.** Let $\alpha_1, \cdots, \alpha_{n-1}$ represent $n-1$ real positive numbers. The problem of finding $n-1$ rational fractions $x_1/z, \cdots, x_{n-1}/z$, having a common denominator, which are close approximations to the quantities α, has been solved by Hermite,* Kronecker,† and Minkowski,‡ and for $n=2$ by Hurwitz.§ We shall prove a theorem giving slightly closer limits, except for $n=2$, than those obtained by these writers.

Consider the linear forms

$$y_1 \equiv x_1 - \alpha_1 z, \quad y_2 \equiv x_2 - \alpha_2 z, \quad \cdots, \quad y_{n-1} \equiv x_{n-1} - \alpha_{n-1} z.$$

In the n-space $(y_1, \cdots, y_{n-1}, z)$ construct the lattice-points obtained by substituting all possible integers for $x_1, \cdots, x_{n-1}, z$. Construct also the planes

$$y_1 = a_1 + h_1, \quad \cdots, \quad y_{n-1} = a_{n-1} + h_{n-1}, \quad z = \tfrac{1}{2} + kh_n.$$

Here k is a given positive integer; $a_1, \cdots, a_{n-1}$ any set of $n-1$ numbers *not* representable by the forms $y_1, \cdots, y_{n-1}$; while $h_1, \cdots, h_{n-1}$ run, independently of each other, through all integers from $-\infty$ to $+\infty$. These planes divide the n-space into fundamental parallelepipeds, each of volume $W = k$, and each containing just k lattice-points. For there are just k sets of integers $x_1, \cdots, x_{n-1}, z$ which satisfy the inequalities

$$a_i + h_i < x_i - \alpha_i z < a_i + h_i + 1 \qquad (i = 1, \cdots, n-1),$$

$$\tfrac{1}{2} + kh_n < z < \tfrac{1}{2} + k(h_n + 1).$$

We now apply Theorem I, where S represents the continuum of points satisfying the conditions

$$|z| < a;$$

$$(6) \quad \left|\frac{y_i}{b}\right| + \left|\frac{2^n (n-1)^{n-1} z}{n^n a}\right| < 1 \quad \text{when} \quad \left|\frac{z}{a}\right| \leqq \left(\frac{n}{2(n-1)}\right)^{n-1},$$

$$\left|\frac{z}{a}\right|\left(\left|\frac{y_i}{b}\right| + 1\right)^{n-1} < 1 \quad \text{when} \quad 1 > \left|\frac{z}{a}\right| > \left(\frac{n}{2(n-1)}\right)^{n-1}$$

$$(i = 1, \cdots, n-1).$$

Here a and b are two positive real numbers subject to the restrictions

$$(7) \quad ab^{n-1}\left\{\frac{n^{n-1}}{(n-1)^{n-1}} - \frac{(n-2)^n}{(n-1)^{n-1} n} + 2^n (n-1) \int_0^{1-2/n} \frac{v^{n-1}\, dv}{(1+v)^n}\right\} = 1, \quad b < \frac{1}{2}.$$

* Journal für Mathematik, vol. 40 (1850), p. 266.

† *Werke*, Bd. I, p. 636.

‡ *Geometrie der Zahlen*, p. 108 ff.

§ Mathematische Annalen, vol. 39 (1891), p. 279.

The volume of S is $V = 1$ by (7). We can therefore apply a translation

$$y_1' = y_1 + \delta_1, \quad \cdots, \quad y_{n-1}' = y_{n-1} + \delta_{n-1}, \quad z' = z + \delta_n$$

to S which will bring it into such a position that two lattice-points, $(y_{11}, \cdots, y_{1\,n-1}, z_1)$, $(y_{21}, \cdots, y_{2\,n-1}, z_2)$ are contained in S, or lie as near as we wish to its boundary.

The two integers z_1, z_2 cannot be equal. For otherwise

$$|x_{1i} - x_{2i}| = |y_{1i} - y_{2i}| = |(y_{1i} - \delta_i) - (y_{2i} - \delta_i)| < 2b + \epsilon < 1,$$

by (6) and (7), i. e., $x_{1i} - x_{2i} = 0$ for every subscript i, and hence the two lattice-points would not be distinct. If we therefore set

$$X_1 = x_{11} - x_{21}, \quad \cdots, \quad X_{n-1} = x_{1\,n-1} - x_{2\,n-1}, \quad Z = z_1 - z_2,$$

we have $Z \geqq 1$, and we can prove that

$$|X_i - \alpha_i Z| < 2b + \epsilon_1, \qquad |X_i - \alpha_i Z|\,|Z|^{1/n-1} < a^{1/n-1} b + \epsilon_2,$$

where ϵ_1 and ϵ_2 are quantities as small as we please. If now we notice that from (7)

$$ab^{n-1}\left(\frac{n}{n-1}\right)^{n-1}\left[1 + \left(\frac{n-2}{n}\right)^{n-2}\right] \leqq 1,$$

and that z may be assumed positive, these results give at once:

THEOREM IV. *Given $n - 1$ positive quantities $\alpha_1, \cdots, \alpha_{n-1}$, and an arbitrarily small quantity $b < \frac{1}{2}$, we can find n integers $X_1, \cdots, X_{n-1}, Z$ such that the $n - 1$ differences*

$$\left|\frac{X_i}{Z} - \alpha_i\right|$$

are not greater than $2b$, and at the same time are all not greater than

$$\frac{\gamma}{Z^{n/n-1}} = \frac{(n-1)\,Z^{-(n/n-1)}}{n\left[1 + \left(\frac{n-2}{n}\right)^{n+2}\right]^{1/n-1}}.$$

The common denominator Z need not be taken greater than $2a \leqq 2\,(\gamma / b)^{n-1}$.

For $n = 2$, Hurwitz proved (l. c.) that $\gamma = 1/\sqrt{5}$, and Minkowski* proved that, for $n \geqq 2$, $\gamma < (n-1)/n$. For large values of n, this may be written $\gamma = e^{-1/n}$, while the expression for γ in Theorem IV becomes $(e + 1/e)^{-1/n}$.

* *Geometrie der Zahlen*, p. 112.