ACTA ARITHMETICA
XXVII (1975)

Irregularities of distribution IX *

by

WOLFGANG M. SCHMIDT (Boulder, Colo.)

Yu. V. Linnik in memoriam

1. Introduction. Let U^k be the k-dimensional unit cube $0 \leqslant x_1 \leqslant 1, \ldots, 0 \leqslant x_k \leqslant 1$, and let $\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_N$ be points in U^k. There are many ways to measure the "irregularity" of the distribution of these N points.

Given a Lebesgue measurable subset A of U^k with measure $\mu(A)$, write $z(A)$ for the number of the given N points which lie in A, and put

$$D(A) = z(A) - N\mu(A).$$

If $\mathfrak{A}$ is a non-empty class of measurable sets in U^k, write

$$D(\mathfrak{A}) = \sup |D(A)|,$$

where the supremum is over all $A \in \mathfrak{A}$. Further put

$$\Delta(\mathfrak{A}) = D(\mathfrak{A})/N.$$

One could call $\Delta(\mathfrak{A})$ the *discrepancy with respect to* $\mathfrak{A}$ of the given N points. It is clear that $0 \leqslant \Delta(\mathfrak{A}) \leqslant 1$.

By a *box* we shall understand a set of the type $a_1 \leqslant x_1 \leqslant b_1, \ldots, a_k \leqslant x_k \leqslant b_k$. Let $\mathfrak{J}$ be the class of boxes in U^k, $\mathfrak{W}$ the class of closed cubes in U^k with sides parallel to the coordinate axes, $\mathfrak{B}$ the class of closed balls in U^k, and $\mathfrak{C}$ the class of convex subsets of U^k.

It is known that $\Delta(\mathfrak{J}) \geqslant c_1(k) N^{-1} (\log N)^{(k-1)/2}$ (K.F. Roth [4]), that $\Delta(\mathfrak{J}) \geqslant c_2 N^{-1} \log N$ if $k = 2$ (W. M. Schmidt [6]), that $\Delta(\mathfrak{B}) \geqslant c_3(k, \varepsilon) N^{((k-1)/2k(k+2))-1-\varepsilon}$ for $\varepsilon > 0$ (W. M. Schmidt [5], Corollary to Theorem 3A), and that $\Delta(\mathfrak{C}) \geqslant c_4(k) N^{-(k+1)/(2k)}$ (S.K. Zaremba [9]). We shall improve the last one of these estimates:

THEOREM 1. $\Delta(\mathfrak{C}) \geqslant c_5(k) N^{-2/(k+1)}$.

---

* Written with partial support from NSF grant NSF-GP-33026X. The paper may be read independently of the preceding papers of this series.

Since $\mathfrak{A} \subseteq \mathfrak{A}'$ *implies* $\Delta(\mathfrak{A}) \leqslant \Delta(\mathfrak{A}')$, *we have*

$$\Delta(\mathfrak{W}) \leqslant \Delta(\mathfrak{J}) \leqslant \Delta(\mathfrak{C}), \qquad \Delta(\mathfrak{B}) \leqslant \Delta(\mathfrak{C}).$$

On the other hand, according to E. Hlawka [2] (see also [1]), we have

$$(1) \qquad \Delta(\mathfrak{C}) \leqslant c_6(k)\,\Delta(\mathfrak{J})^{1/k},$$

$$(2) \qquad \Delta(\mathfrak{C}) \leqslant c_7(k)\,\Delta(\mathfrak{W})^{1/(k+1)},$$

$$(3) \qquad \Delta(\mathfrak{C}) \leqslant c_8(k)\,|\log \Delta(\mathfrak{B})|^{-c_9(k)}.$$

A wide generalization of (1) was given by R. Mück and W. Philipp [3]. It was shown by S. K. Zaremba [9] that the exponent $1/k$ in (1) is best possible. J. W. S. Cassels (unpublished) showed that $\Delta(\mathfrak{J}) \leqslant c_{10}(k)\,\Delta(\mathfrak{B})^{1/(k+1)}$, and C.J. Smyth [7] generalized this to

$$(4) \qquad \Delta(\mathfrak{C}) \leqslant c_{11}(k)\,\Delta(\mathfrak{B})^{1/(k+1)},$$

which is an improvement over (3). He also showed [8] that

$$\Delta(\mathfrak{J}) \leqslant c_{12}(k)\,\Delta(\mathfrak{B})^{1/k}\big(1+|\log \Delta(\mathfrak{B})|\big)^{c_{13}(k)}.$$

We shall improve (2) and (4). Write $\exp x = e^x$.

THEOREM 2.

$$\Delta(\mathfrak{C}) \leqslant c_{14}(k)\,\Delta(\mathfrak{W})^{1/k}.$$

THEOREM 3.

$$\Delta(\mathfrak{C}) \leqslant c_{15}(k)\,\Delta(\mathfrak{B})^{1/k}\exp\big(2(\log 2)^{1/2}k^{-1}|\log \Delta(\mathfrak{B})|^{1/2}\big).$$

In particular, it follows that

$$\Delta(\mathfrak{C}) \leqslant c_{16}(k,\varepsilon)\,\Delta(\mathfrak{B})^{(1/k)-\varepsilon}$$

for $\varepsilon > 0$.

2. Proof of Theorem 1. We may suppose $k > 1$. Let B be the ball of radius $\frac{1}{2}$ contained in U^k, and let S be the surface of B. Let C be a closed spherical cap on S with spherical radius ϱ. (With the radius normalized such that a half sphere has radius $\pi/2$.) The convex hull $\bar{C}$ of C is a solid spherical cap. For $0 < \varrho < \pi/2$, $\mu(\bar{C})$ is a continuous function of ϱ with[1]

$$(5) \qquad c_1\varrho^{k+1} < \mu(\bar{C}) < c_2\varrho^{k+1}.$$

If N is sufficiently large, there is a number ϱ_0 such that a cap C of spherical radius ϱ_0 has

$$\mu(\bar{C}) = \frac{1}{2N}.$$

[1] We start the numbering of constants $c_1, c_2, \ldots$ anew in each section, except in the last one. These constants may depend on the dimension k.

In view of (5), $0 < \varrho_0 < c_3N^{-1/(k+1)}$. We now pick as many pairwise disjoint caps with radius ϱ_0 as possible; say $C_1, \ldots, C_M$. For large N and hence small ϱ_0 we have $M \geqslant c_4\varrho_0^{-(k-1)}$, whence

$$(6) \qquad M \geqslant c_5N^{(k-1)/(k+1)}.$$

Given a sequence of numbers $\sigma_1, \ldots, \sigma_M$, with each σ_i either $+1$ or -1, let $B(\sigma_1, \ldots, \sigma_M)$ consist of all $\boldsymbol{x} \in B$ which do not lie in a cap $\bar{C}_i$ with $\sigma_i = -1$. In other words, $B(\sigma_1, \ldots, \sigma_M)$ is obtained from B by removing the solid caps $\bar{C}_i$ for which $\sigma_i = -1$.

Now the function $D(A)$ is *additive*, i.e. it satisfies

$$D(A \cup A') = D(A) + D(A')$$

if $A \cap A' = \emptyset$. It follows easily that

$$D\big(B(\sigma_1, \ldots, \sigma_M)\big) - D\big(B(-\sigma_1, \ldots, -\sigma_M)\big) = \sum_{i=1}^{M} \sigma_i D(\bar{C}_i).$$

We have

$$D(\bar{C}_i) = z(\bar{C}_i) - N\mu(\bar{C}_i) = z(\bar{C}_i) - \tfrac{1}{2}.$$

Hence for every i, either $D(\bar{C}_i) \geqslant \frac{1}{2}$ or $D(\bar{C}_i) \leqslant -\frac{1}{2}$. Choose σ_i such that $\sigma_i D(\bar{C}_i) \geqslant \frac{1}{2}$ $(1 \leqslant i \leqslant M)$. Then

$$D\big(B(\sigma_1, \ldots, \sigma_M)\big) - D\big(B(-\sigma_1, \ldots, -\sigma_M)\big) \geqslant \tfrac{1}{2}M,$$

and either $A = B(\sigma_1, \ldots, \sigma_M)$ or $A = B(-\sigma_1, \ldots, -\sigma_M)$ has $|D(A)| \geqslant \frac{1}{4}M$. Thus by (6),

$$\Delta(\mathfrak{C}) \geqslant \tfrac{1}{4}M/N \geqslant c_6N^{-2/(k+1)}.$$

Theorem 1 is proven.

The following is of interest in this connection. Let $\mathfrak{Q}$ be the class of subsets Q of U^k such that if $(y_1, \ldots, y_k) \in Q$, then every $(x_1, \ldots, x_k)$ with $0 \leqslant x_i \leqslant y_i$ $(i = 1, \ldots, k)$ also lies in Q. Then

$$(7) \qquad \Delta(\mathfrak{Q}) \geqslant c_7N^{-1/k}.$$

For let G consist of points in U^k with $x_1 + \ldots + x_k \leqslant 1$, and H of points with $x_1 + \ldots + x_k = 1$. Let $0 < \delta < 1/k$ and let $\boldsymbol{x} = (x_1, \ldots, x_k)$ be a point on H with $(k-1)\delta < x_i \leqslant 1 - \delta$ $(i = 1, \ldots, k)$. Let $Q(\boldsymbol{x})$ consist of points $\boldsymbol{y} = (y_1, \ldots, y_k)$ with

$$y_1 + \ldots + y_k > 1 \quad \text{and} \quad y_i \leqslant x_i + \delta \quad (i = 1, \ldots, k).$$

Then $Q(\boldsymbol{x})$ lies in U^k and has volume $\mu\big(Q(\boldsymbol{x})\big) = (2k)^k/k!$. If N is sufficiently large, we may choose δ such that this volume equals $1/(2N)$. Then $\delta \leqslant c_8N^{-1/k}$.

Pick as many pairwise disjoint sets $Q(x)$ as possible; say $Q_1, \ldots, Q_M$. Clearly $M \geqslant c_9 \delta^{-(k-1)}$, whence

$$M \geqslant c_{10} N^{(k-1)/k}.$$

For any sequence $\sigma_1, \ldots, \sigma_M$ of $+1$ and -1 signs, let $Q(\sigma_1, \ldots, \sigma_M)$ be the union of G with the "blisters" Q_i for which $\sigma_i = 1$. The set $Q(\sigma_1, \ldots, \sigma_M)$ belongs to $\mathfrak{Q}$. We have

$$D\big(Q(\sigma_1, \ldots, \sigma_M)\big) - D\big(Q(-\sigma_1, \ldots, -\sigma_M)\big) = \sum_{i=1}^{M} \sigma_i D(Q_i).$$

By an argument used in the proof of Theorem 1, we obtain a set $A \in \mathfrak{Q}$ with

$$|D(A)|/N \geqslant \tfrac{1}{4} M/N \geqslant c_7 N^{-1/k}.$$

3. Proof of Theorem 2. Let $B(\boldsymbol{c}, \varrho)$ be the closed ball with center $\boldsymbol{c}$ and radius ϱ. Given a subset S of U^k, let $S(\varrho)$ consist of points $\boldsymbol{x}$ for which $B(\boldsymbol{x}, \varrho) \subseteq S$. Let S' consist of $\boldsymbol{x} \in U^k$ which are not in S.

For each $\sigma > 0$, let $\mathfrak{S}(\sigma)$ be the class of subsets S of U^k having

$$(8) \qquad \mu\big(S(\varrho)\big) \geqslant \mu(S) - \varrho\sigma, \qquad \mu\big(S'(\varrho)\big) \geqslant \mu(S') - \varrho\sigma$$

for every $\varrho > 0$.

LEMMA 1. *There is a constant $c_1 = c_1(k)$ such that*

$$\mathfrak{C} \subseteq \mathfrak{S}(c_1).$$

The proof may be left to the reader. Incidentally, it may be shown that $\mathfrak{Q} \subseteq \mathfrak{S}(c_1')$. It is now clear that Theorem 2 is a consequence of

THEOREM 2a.

$$\Delta\big(\mathfrak{S}(\sigma)\big) \leqslant c_2(k, \sigma)\, \Delta(\mathfrak{W})^{1/k}.$$

Proof. Let $S[\varrho]$ consist of points $\boldsymbol{x} \in U^k$ which have a distance $< \varrho$ from the boundary of S. Every $\boldsymbol{x} \in S[\varrho]$ is either in S but not in $S(\varrho)$, or is in S' but not in $S'(\varrho)$. Hence for $S \in \mathfrak{S}(\sigma)$,

$$\mu(S[\varrho]) \leqslant 2\varrho\sigma.$$

Now if $k = 1$ and if $z_1, \ldots, z_M$ are on the boundary of S and in the interior of U, then for small ϱ, $S[\varrho]$ contains the M open intervals with centers $z_1, \ldots, z_M$ and of length 2ϱ. Hence for small ϱ, $\mu(S[\varrho]) \geqslant 2\varrho M$, and we get $M \leqslant \sigma$. Thus S has at most $\sigma + 2$ boundary points, and is therefore the union a bounded number of points and intervals. Hence Theorem 2a is true for $k = 1$.

We may henceforth assume that $k > 1$. Pick a point $\boldsymbol{a} = (a_1, \ldots, a_k)$ such that for each of the given points $\boldsymbol{p}_i$ $(i = 1, \ldots, N)$, each coordinate of $\boldsymbol{p}_i - \boldsymbol{a}$ is irrational. For a positive integer n, let $\mathfrak{W}(n)$ be the class of cubes

$$a_i + \frac{u_i}{n} \leqslant x_i \leqslant a_i + \frac{u_i + 1}{n} \qquad (i = 1, \ldots, k)$$

with integers $u_1, \ldots, u_k$. Let $\mathfrak{V}(n)$ be the set of cubes of $\mathfrak{W}(n)$ which are contained in S. Since a cube of $\mathfrak{W}(n)$ has diameter $k^{1/2}/n$, it follows that the cubes of $\mathfrak{V}(n)$ cover $S(k^{1/2}/n)$, and their number $\nu(n)$ satisfies

$$(9) \qquad n^k \mu(S) \geqslant \nu(n) \geqslant n^k \mu\big(S(k^{1/2}/n)\big) \geqslant n^k \mu(S) - n^{k-1} \sigma k^{1/2}.$$

For each positive integer i, the union of the cubes of $\mathfrak{V}(2^i)$ contains the union of the cubes of $\mathfrak{V}(2^{i-1})$. Put $\mathfrak{V}_1 = \mathfrak{V}(2^1)$, and for $i \geqslant 2$, let $\mathfrak{V}_i$ consist of the cubes of $\mathfrak{V}(2^i)$ which are not contained in a cube of $\mathfrak{V}(2^{i-1})$. If ν_i is the number of cubes in $\mathfrak{V}_i$, then $\nu_1 = \nu(2)$, and for $i \geqslant 2$ we have

$$2^{-ik} \nu_i + 2^{-(i-1)k} \nu(2^{i-1}) \leqslant \mu(S),$$

whence by (9),

$$\nu_i \leqslant 2^{ik} \mu(S) - 2^k \nu(2^{i-1}) \leqslant \sigma k^{1/2} 2^{i(k-1)+1}.$$

Since any two distinct cubes in any of the sets $\mathfrak{V}_1, \mathfrak{V}_2, \ldots$ are disjoint except possibly for their boundaries, and since by our choice of $\boldsymbol{a}$ none of the given N points lie on such a boundary, we have for every positive integer M,

$$\begin{aligned} z(S) &\geqslant \sum_{i=1}^{M} \sum_{W \in \mathfrak{V}_i} z(W) \geqslant \sum_{i=1}^{M} \sum_{W \in \mathfrak{V}_i} \big(N\mu(W) - N\Delta(\mathfrak{W})\big) \\ &= N\Big(\Big(\sum_{W \in \mathfrak{V}(2^M)} \mu(W)\Big) - \Delta(\mathfrak{W}) \sum_{i=1}^{M} \nu_i\Big) \\ &\geqslant N\Big(\mu\big(S(k^{1/2} 2^{-M})\big) - \Delta(\mathfrak{W})\Big(2^k + \sigma k^{1/2} \sum_{i=2}^{M} 2^{i(k-1)+1}\Big)\Big) \\ &\geqslant N\mu(S) - Nc_3(k, \sigma)\big(2^{-M} + \Delta(\mathfrak{W}) 2^{M(k-1)}\big), \end{aligned}$$

since $k > 1$. Now if we choose M such that $2^{M-1} \leqslant \Delta(\mathfrak{W})^{-1/k} < 2^M$, then

$$z(S) - N\mu(S) \geqslant -Nc_3(k, \sigma)\Delta(\mathfrak{W})^{1/k}(1 + 2^{k-1}) = -Nc_2(k, \sigma)\Delta(\mathfrak{W})^{1/k}.$$

This inequality remains true if we replace S by S'. Hence

$$|z(S) - N\mu(S)| \leqslant Nc_2(k, \sigma)\Delta(\mathfrak{W})^{1/k},$$

and Theorem 2a follows.

4. Successive sweeping. Given a set A, let $rA + \boldsymbol{y}$ be the set of points $r\boldsymbol{a} + \boldsymbol{y}$ with $\boldsymbol{a} \in A$. Let $\mathfrak{A}(A)$ be the class of sets $rA + \boldsymbol{y}$ with $r > 0$ which are contained in U^k. In view of Lemma 1, Theorem 3 is a consequence of

THEOREM 3a. *Suppose $A \in \mathfrak{S}(\tau)$ for some τ, and suppose $\mu(A) > 0$. Then for every $\sigma > 0$,*

$$\Delta(\mathfrak{S}(\sigma)) \leqslant c_1(A, \sigma)\Delta(\mathfrak{A}(A))^{1/k}\exp\left(2(\log 2)^{1/2}k^{-1}|\log \Delta(\mathfrak{A}(A))|^{1/2}\right).$$

Denote the distance of points $\boldsymbol{x}, \boldsymbol{y}$ by

$$|\boldsymbol{x}-\boldsymbol{y}|.$$

Now let $r_1, r_2, \ldots,$ be positive reals with

$$r_{i+1} \leqslant \tfrac{1}{2}r_i \quad (i = 1, 2, \ldots), \tag{10}$$

and set $s_i = k^{1/2}r_i$. The set r_iA has diameter $\leqslant s_i$.

For a set T, let $\chi(T|\boldsymbol{x})$ be the characteristic function of T. Let S be a set belonging to $\mathfrak{S}(\sigma)$.

We are going to construct functions $f_\nu(\boldsymbol{x}), g_\nu(\boldsymbol{x}), h_\nu(\boldsymbol{x})$ $(\nu = 0, 1, 2, \ldots)$. We begin by setting

$$f_0(\boldsymbol{x}) = 0.$$

If a continuous function $f_\nu(\boldsymbol{x})$ is given, write

$$g_\nu(\boldsymbol{x}) = \chi(S|\boldsymbol{x}) - f_\nu(\boldsymbol{x}),$$

$$h_\nu(\boldsymbol{x}) = \min_{|\boldsymbol{y}-\boldsymbol{x}| \leqslant s_{\nu+1}} g_\nu(\boldsymbol{y}),$$

$$f_{\nu+1}(\boldsymbol{x}) = f_\nu(\boldsymbol{x}) + \left(\mu(r_{\nu+1}A)\right)^{-1}\int \chi(r_{\nu+1}A + \boldsymbol{y}|\boldsymbol{x})h_\nu(\boldsymbol{y})\,d\boldsymbol{y}.$$

LEMMA 2. *We have*

(i) $\quad 0 \leqslant f_{\nu-1}(\boldsymbol{x}) \leqslant f_\nu(\boldsymbol{x}) \leqslant \chi(S|\boldsymbol{x}) \quad (\nu = 1, 2, \ldots),$

(iia) $\quad |f_\nu(\boldsymbol{x}) - f_\nu(\boldsymbol{x}')| \leqslant c_2(A)r_\nu^{-1}|\boldsymbol{x}-\boldsymbol{x}'| \quad (\nu = 1, 2, \ldots),$

and in particular $f_\nu(\boldsymbol{x})$ is continuous.

(iib) $\quad |f_\nu(\boldsymbol{x}) - f_\nu(\boldsymbol{x}')| \leqslant 2^{\nu-i}c_2(A)r_i^{-1}|\boldsymbol{x}-\boldsymbol{x}'|$

if $1 \leqslant i \leqslant \nu-1$ and if $|\boldsymbol{x}-\boldsymbol{x}'| \leqslant s_\nu$ and $\boldsymbol{x}, \boldsymbol{x}' \in S(3(s_{i+1}+\ldots+s_\nu))$.

(iiia) $\quad f_\nu(\boldsymbol{x}) = 1 \quad$ *if* $\quad \boldsymbol{x} \in S(2s_1) \quad (\nu = 1, 2, \ldots),$

(iiib) $\quad f_\nu(\boldsymbol{x}) \geqslant 1 - 2^{\nu-i}c_3(A)(s_\nu/s_i)$

if $1 \leqslant i \leqslant \nu-1$ and $\boldsymbol{x} \in S(6s_{i+1})$.

Our construction may be interpreted as follows. We first sweep S with a broom of the size and shape of r_1A. We can sweep the middle of S, more precisely $S(2s_1)$, very well. But we cannot sweep the border areas of S very well. We then take a smaller broom of the size and shape of r_2A. And so on. We obtain a better and better sweeping of S which is expressed by (i) and (iiib). But it would have been inefficient to sweep right away with a very small broom of the size and shape of $r_\nu A$.

Proof. We proceed by induction on ν. Assume that either $\nu = 0$ or that the lemma is true for a particular value of $\nu > 0$. We have $0 \leqslant f_\nu(\boldsymbol{x}) \leqslant \chi(S|\boldsymbol{x})$, whence $0 \leqslant g_\nu(\boldsymbol{x}) \leqslant \chi(S|\boldsymbol{x})$. Now if $\boldsymbol{x} \in r_{\nu+1}A + \boldsymbol{y}$, then $\boldsymbol{x}-\boldsymbol{y} \in r_{\nu+1}A$, whence $|\boldsymbol{y}-\boldsymbol{x}| \leqslant s_{\nu+1}$, whence $h_\nu(\boldsymbol{y}) \leqslant g_\nu(\boldsymbol{x})$. We obtain

$$0 \leqslant \int \chi(r_{\nu+1}A + \boldsymbol{y}|\boldsymbol{x})h_\nu(\boldsymbol{y})\,d\boldsymbol{y} \leqslant g_\nu(\boldsymbol{x})\int \chi(r_{\nu+1}A + \boldsymbol{y}|\boldsymbol{x})\,d\boldsymbol{y} = g_\nu(\boldsymbol{x})\mu(r_{\nu+1}A),$$

and

$$f_\nu(\boldsymbol{x}) \leqslant f_{\nu+1}(\boldsymbol{x}) \leqslant f_\nu(\boldsymbol{x}) + g_\nu(\boldsymbol{x}) = \chi(S|\boldsymbol{x}).$$

Hence (i) is true for $\nu+1$.

Now it is clear that $l_{\nu+1}(\boldsymbol{x}) = f_{\nu+1}(\boldsymbol{x}) - f_\nu(\boldsymbol{x})$ has

$$l_{\nu+1}(\boldsymbol{x}) - l_{\nu+1}(\boldsymbol{x}') = \left(\mu(r_{\nu+1}A)\right)^{-1}\int\left(\chi(r_{\nu+1}A + \boldsymbol{y}|\boldsymbol{x}) - \chi(r_{\nu+1}A + \boldsymbol{y}|\boldsymbol{x}')\right)h_\nu(\boldsymbol{y})\,d\boldsymbol{y}.$$

Since $0 \leqslant h_\nu(\boldsymbol{y}) \leqslant 1$, we obtain

$$l_{\nu+1}(\boldsymbol{x}) - l_{\nu+1}(\boldsymbol{x}') \leqslant \left(\mu(r_{\nu+1}A)\right)^{-1}\mu(C_1),$$

where C_1 consists of $\boldsymbol{y}$ for which $-\boldsymbol{y}$ lies in $r_{\nu+1}A - \boldsymbol{x}$ but not in $r_{\nu+1}A - \boldsymbol{x}'$. Now

$$\mu(C_1) = r_{\nu+1}^k\mu(C_2),$$

where C_2 consists of $\boldsymbol{y}$ which are in $A - r_{\nu+1}^{-1}(\boldsymbol{x}-\boldsymbol{x}')$ but not in A. Now if $\boldsymbol{y} \in C_2$ lies in U^k, then $\boldsymbol{y} \in A'$ and $\boldsymbol{y} \notin A'(r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'|)$. Hence by virtue of $A \in \mathfrak{S}(\tau)$, the intersection $C_2 \cap U^k$ has volume $\leqslant \tau r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'|$. On the other hand if $\boldsymbol{y} \in C_2$ lies outside of U^k, then it has distance $\leqslant r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'|$ from U^k, and if $r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'| \leqslant 1$, then the part of C_2 outside U^k has volume $\leqslant 3^k r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'|$. Thus if $|\boldsymbol{x}-\boldsymbol{x}'|$ is small, then $\mu(C_2) \leqslant (\tau+3^k)r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'|$, and therefore

$$l_{\nu+1}(\boldsymbol{x}) - l_{\nu+1}(\boldsymbol{x}') \leqslant \tfrac{1}{2}c_2(A)r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'|,$$

with $c_2(A) = 2\mu(A)^{-1}(\tau+3^k)$. It follows that for *every* $\boldsymbol{x}, \boldsymbol{x}'$,

$$|l_{\nu+1}(\boldsymbol{x}) - l_{\nu+1}(\boldsymbol{x}')| \leqslant \tfrac{1}{2}c_2(A)r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'|. \tag{11}$$

Now if $\nu = 0$, we have $f_{\nu+1}(\boldsymbol{x}) = f_1(\boldsymbol{x}) = l_1(\boldsymbol{x})$, and the case $\nu = 1$ of (iia) follows. If $\nu > 0$, we use our inductive assumption, (10), (11) and the relation $f_{\nu+1}(\boldsymbol{x}) = f_\nu(\boldsymbol{x}) + l_{\nu+1}(\boldsymbol{x})$ to obtain

$$|f_{\nu+1}(\boldsymbol{x}) - f_{\nu+1}(\boldsymbol{x}')| \leqslant \left(c_2(A)r_\nu^{-1} + \tfrac{1}{2}c_2(A)r_{\nu+1}^{-1}\right)|\boldsymbol{x}-\boldsymbol{x}'| \leqslant c_2(A)r_{\nu+1}^{-1}|\boldsymbol{x}-\boldsymbol{x}'|.$$

Thus (iia) is true for $\nu+1$.

Before taking up the proof of (iib) we observe the following. Suppose that either

(12) $$i = \nu \quad \text{and} \quad z, z' \in S(s_{\nu+1}),$$

or that

(13) $$1 \leqslant i \leqslant \nu-1, \quad |z-z'| \leqslant s_\nu \quad \text{and} \quad z, z' \in S\big(3(s_{i+1}+\ldots+s_\nu)+s_{\nu+1}\big).$$

Now $h_\nu(z)$ equals $g_\nu(w)$ for some w with $|w-z| \leqslant s_{\nu+1}$. Since $h_\nu(z')$ is defined as the minimum of $g_\nu(u)$ for $|u-z'| \leqslant s_{\nu+1}$, and since $w' = w+ +z'-z$ has $|w'-z'| \leqslant s_{\nu+1}$, we get $h_\nu(z') \leqslant g_\nu(w')$, whence

(14) $$h_\nu(z')-h_\nu(z) \leqslant g_\nu(w')-g_\nu(w).$$

Our hypotheses on z, z' imply that $w, w' \in S$, whence $\chi(S|w) = \chi(S|w') = 1$ and

(15) $$g_\nu(w')-g_\nu(w) = f_\nu(w)-f_\nu(w').$$

Now if (12) holds, apply (iia) to w, w'. On the other hand, if (13) holds, then $|w-w'| = |z-z'| \leqslant s_\nu$ and $w, w' \in S\big(3(s_{i+1}+\ldots+s_\nu)\big)$. In this case we apply (iib) to w, w'. We may do so, since (iib) is true for our particular value of ν by induction. In either case, we get

$$|f_\nu(w)-f_\nu(w')| \leqslant 2^{\nu-i}c_2(A)r_i^{-1}|w-w'| = 2^{\nu-i}c_2(A)r_i^{-1}|z-z'|.$$

Combining this with (14) and (15), we may conclude that both (12) or (13) implies

$$|h_\nu(z')-h_\nu(z)| \leqslant 2^{\nu-i}c_2(A)r_i^{-1}|z-z'|.$$

Now suppose that $1 \leqslant i \leqslant \nu$, that $|x-x'| \leqslant s_{\nu+1}$ and that $x, x' \in S\big(3(s_{i+1}+\ldots+s_{\nu+1})\big)$. We have

$$l_{\nu+1}(x)-l_{\nu+1}(x') = \big(\mu(r_{\nu+1}A)\big)^{-1}\int\chi(r_{\nu+1}A+y|x')\big(h_\nu(y+x-x')-h_\nu(y)\big)dy.$$

The integrand is zero unless $|y-x'| \leqslant s_{\nu+1}$, hence is zero unless $y \in S\big(3(s_{i+1}+ +\ldots+s_\nu)$[2]$+2s_{\nu+1}\big)$. But then $y+x-x' \in S\big(3(s_{i+1}+\ldots+s_\nu)+s_{\nu+1}\big)$. We apply the remark made above to $z = y$, $z' = y+x-x'$, and we obtain

$$|h_\nu(y+x-x')-h_\nu(y)| \leqslant 2^{\nu-i}c_2(A)r_i^{-1}|x-x'|.$$

Hence

$$|l_{\nu+1}(x)-l_{\nu+1}(x')| \leqslant 2^{\nu-i}c_2(A)r_i^{-1}|x-x'|.$$

Since $f_{\nu+1}(x) = f_\nu(x)+l_{\nu+1}(x)$ and since

$$|f_\nu(x)-f_\nu(x')| \leqslant 2^{\nu-i}c_2(A)r_i^{-1}|x-x'|$$

(2) The empty sum occurring when $i = \nu$ is to be interpreted as zero.

by induction, we obtain

$$|f_{\nu+1}(x)-f_{\nu+1}(x')| \leqslant 2^{\nu+1-i}c_2(A)r_i^{-1}|x-x'|.$$

Thus (iib) is true for $\nu+1$.

We have

$$f_1(x) = \mu(r_1A)^{-1}\int\chi(r_1A+y|x)h_0(y)dy.$$

If $x \in S(2s_1)$ and if $x \in r_1A+y$, then $|y-x| \leqslant s_1$ and $y \in S(s_1)$. Since g_0 is the characteristic function of S, the definition of $h_0(y)$ implies that $h_0(y) = 1$ for $y \in S(s_1)$. Therefore $x \in S(2s_1)$ implies that $f_1(x) = 1$. Since $f_1(x) \leqslant f_\nu(x) \leqslant 1$ by (i), we obtain (iiia).

There remains (iiib). Suppose $1 \leqslant i \leqslant \nu$ and $x \in S\big(3(s_{i+1}+\ldots+s_{\nu+1})\big)$. We have

(16) $$f_{\nu+1}(x) = \big(\mu(r_{\nu+1}A)\big)^{-1}\int\chi(r_{\nu+1}A+y|x)\big(f_\nu(x)+h_\nu(y)\big)dy.$$

Here $h_\nu(y) = g_\nu(w)$ for some w with $|w-y| \leqslant s_{\nu+1}$. In particular, if $x \in r_{\nu+1}A+y$, we have $|y-x| \leqslant s_{\nu+1}$, whence $|w-x| \leqslant 2s_{\nu+1}$. In particular $w \in S$, so that $g_\nu(w) = 1-f_\nu(w)$ and

$$f_\nu(x)+h_\nu(y) = 1+f_\nu(x)-f_\nu(w).$$

Now either $i = \nu$; then we estimate $f_\nu(x)-f_\nu(w)$ by (iia). Or $i \leqslant \nu-1$, $|w-x| \leqslant 2s_{\nu+1} \leqslant s_\nu$, and both $x, w \in S\big(3(s_{i+1}+\ldots+s_\nu)\big)$. Then we estimate $f_\nu(x)-f_\nu(w)$ by (iib). In either case we get

$$|f_\nu(x)-f_\nu(w)| \leqslant 2^{\nu-i}c_2(A)r_i^{-1}|x-w| \leqslant 2^{\nu-i}c_2(A)(2s_{\nu+1}/r_i) = 2^{\nu-i}c_3(A)(s_{\nu+1}/s_i),$$

say. Thus every y with $x \in r_{\nu+1}A+y$ has

$$f_\nu(x)+h_\nu(y) \geqslant 1-2^{\nu-i}c_3(A)(s_{\nu+1}/s_i),$$

and (16) yields

$$f_{\nu+1}(x) \geqslant 1-2^{\nu-i}c_3(A)(s_{\nu+1}/s_i).$$

Since $S(6s_{i+1}) \subseteq S\big(3(s_{i+1}+\ldots+s_{\nu+1})\big)$ by (10), the lemma is proved.

5. A measure on the space $\mathfrak{A}(A)$. Let $r_1, r_2, \ldots$, and $s_1, s_2, \ldots$ be as in § 4. Let M be an integer greater than 1.

The space $\Omega = \mathfrak{A}(A)$ of sets $rA+y$ in U^k may be parametrized by the pair (r, y). We introduce a measure ω on Ω by the formula

$$\int_\Omega a(r, y)d\omega = \sum_{\nu=0}^{M-1}\big(\mu(r_{\nu+1}A)\big)^{-1}\int a(r_{\nu+1}, y)h_\nu(y)dy.$$

This formula is valid for functions $a(r, y)$ on Ω for which the integrals on the right are defined.

LEMMA 3. *We have*

(i) $$\int_\Omega \chi(rA+\boldsymbol{y}|\boldsymbol{x})\,d\omega \leqslant \chi(S|\boldsymbol{x}),$$

(ii) $$\int_\Omega d\omega \leqslant c_4(A,\sigma)(r_1^{-k}+2r_2^{-k}r_1+\ldots+2^{M-1}r_M^{-k}r_{M-1}),$$

(iii) $$\int_\Omega \mu(rA)\,d\omega \geqslant \mu(S)-2^M c_5(A,\sigma)r_M.$$

Proof. We begin by observing that

$$\int_\Omega \chi(rA+\boldsymbol{y}|\boldsymbol{x})\,d\omega = \sum_{\nu=0}^{M-1}\big(\mu(r_{\nu+1}A)\big)^{-1}\int \chi(r_{\nu+1}A+\boldsymbol{y}|\boldsymbol{x})h_\nu(\boldsymbol{y})\,d\boldsymbol{y}$$
$$= \sum_{\nu=0}^{M-1} l_{\nu+1}(\boldsymbol{x}) = f_M(\boldsymbol{x}) \leqslant \chi(S|\boldsymbol{x}).$$

Next,

(17) $$\int_\Omega d\omega = \sum_{\nu=0}^{M-1}\big(\mu(r_{\nu+1}A)\big)^{-1}\int h_\nu(\boldsymbol{y})\,d\boldsymbol{y} \leqslant \sum_{\nu=0}^{M-1}\big(\mu(r_{\nu+1}A)\big)^{-1}\int g_\nu(\boldsymbol{y})\,d\boldsymbol{y}.$$

We have

(18) $$\int g_0(\boldsymbol{y})\,d\boldsymbol{y} = \int \chi(S|\boldsymbol{y})\,d\boldsymbol{y} = \mu(S).$$

For $\nu\geqslant 1$ we write

$$\int g_\nu(\boldsymbol{y})\,d\boldsymbol{y} = \int_{S_1}+\int_{S_2}+\ldots+\int_{S_\nu}+\int_{S_\nu^*},$$

where $S_1 = S(6s_1)$, where S_j is the complement of $S(6s_{j-1})$ in $S(6s_j)$ $(j=2,3,\ldots)$, and where S_ν^* is the complement of $S(6s_\nu)$ in S. By (iiia) of Lemma 2, $g_\nu(\boldsymbol{y}) = 0$ for $\boldsymbol{x}\in S_1$, so that the integral over S_1 is zero. By (iiib) of Lemma 2 we have

$$g_\nu(\boldsymbol{y}) \leqslant 2^{\nu-(j-1)}c_3(A)(s_\nu/s_{j-1})$$

if $\boldsymbol{y}\in S_j$ with $2\leqslant j\leqslant\nu$. On the other hand we have $\mu(S_j)\leqslant 6s_{j-1}\sigma$, because $S\in\mathfrak{S}(\sigma)$. Thus for $2\leqslant j\leqslant\nu$,

$$\int_{S_j} g_\nu(\boldsymbol{y})\,d\boldsymbol{y} \leqslant 6c_3(A)\sigma s_\nu 2^{\nu-j+1}.$$

On S_ν^* we have $g_\nu(\boldsymbol{y})\leqslant 1$, and since $\mu(S_\nu^*)\leqslant 6s_\nu\sigma$, the integral over S_ν^* is $\leqslant 6\sigma s_\nu$. Combining our estimates, we obtain

(19) $$\int g_\nu(\boldsymbol{y})\,d\boldsymbol{y} \leqslant 6\sigma\big(1+c_3(A)\big)s_\nu(2^{\nu-1}+2^{\nu-2}+\ldots+1) < c_5(A,\sigma)2^\nu r_\nu.$$

In view of (17) and (18) we obtain part (ii) of the lemma.

Finally,

$$\int h_\nu(\boldsymbol{y})\,d\boldsymbol{y} = \big(\mu(r_{\nu+1}A)\big)^{-1}\iint \chi(r_{\nu+1}A+\boldsymbol{y}|\boldsymbol{x})h_\nu(\boldsymbol{y})\,d\boldsymbol{x}\,d\boldsymbol{y} = \int l_{\nu+1}(\boldsymbol{x})\,d\boldsymbol{x}.$$

Thus

$$\int_\Omega \mu(rA)\,d\omega = \sum_{\nu=0}^{M-1}\int h_\nu(\boldsymbol{y})\,d\boldsymbol{y} = \sum_{\nu=1}^{M}\int l_\nu(\boldsymbol{x})\,d\boldsymbol{x}$$
$$= \int f_M(\boldsymbol{x})\,d\boldsymbol{x} = \mu(S)-\int g_M(\boldsymbol{x})\,d\boldsymbol{x} \geqslant \mu(S)-2^M c_5(A,\sigma)r_M$$

by (19).

6. Proof of Theorem 3a. We may assume that $\Delta = \Delta(\mathfrak{A}(A))$ is so small that

(20) $$|\log\Delta|/(\log 2) \geqslant 9k^2.$$

Repeated application of Lemma 3 yields

(21) $$z(S) = \sum_{i=1}^{N}\chi(S|\boldsymbol{p}_i) \geqslant \int_\Omega\Big(\sum_{i=1}^{N}\chi(rA+\boldsymbol{y}|\boldsymbol{p}_i)\Big)d\omega = \int_\Omega z(rA+\boldsymbol{y})\,d\omega$$
$$\geqslant \int_\Omega\big(N\mu(rA)-N\Delta(\mathfrak{A}(A))\big)d\omega = N\Big(\int_\Omega \mu(rA)\,d\omega-\Delta\int_\Omega d\omega\Big)$$
$$\geqslant N\big(\mu(S)-2^M c_5(A,\sigma)r_M-\Delta c_4(A,\sigma)R_M\big)$$

with

$$R_M = r_1^{-k}+2r_2^{-k}r_1+\ldots+2^{M-1}r_M^{-k}r_{M-1}.$$

Choose the integer M with

(22) $$M-1 \leqslant |\log\Delta|^{1/2}(\log 2)^{-1/2}k^{-1} < M.$$

Then $M\geqslant 3$ by (20). Let d be the number with

$$\log d = |\log\Delta|/(Mk+1).$$

Now by (20), (22),

$$|\log\Delta|/(Mk+1) \geqslant |\log\Delta|/\big(2|\log\Delta|^{1/2}(\log 2)^{-1/2}+1\big) \geqslant \tfrac{1}{3}|\log\Delta|^{1/2}(\log 2)^{1/2} \geqslant \log 2,$$

so that $d\geqslant 2$.

Put $r_i = d^{-i}$ $(i=1,2,\ldots)$. Then

$$R_M = d^k+2d^{2k-1}+\ldots+2^{M-1}d^{Mk-(M-1)} \leqslant 2^M d^{M(k-1)+1},$$

so that

(23) $$2^M r_M+\Delta R_M \leqslant (2/d)^M(1+\Delta d^{Mk+1}) = 2(2/d)^M,$$

by our choice of d. We have

$$M(\log d - \log 2) = \big(M/(Mk+1)\big)|\log \Delta| - M\log 2$$
$$\geqslant |\log \Delta|\big((1/k) - (1/k^2M)\big) - M\log 2$$
$$\geqslant (1/k)|\log \Delta| - (2/k)|\log \Delta|^{1/2}(\log 2)^{1/2} - \log 2$$

by (22), so that by (23),

$$2^M r_M + \Delta r_M \leqslant 4\Delta^{1/k}\exp\big(2(\log 2)^{1/2}k^{-1}|\log \Delta|^{1/2}\big).$$

This in conjunction with (21) gives

$$z(S) \geqslant N\big(\mu(S) - c_1(A, \sigma)\Delta^{1/k}\exp(\ldots)\big).$$

The same inequality holds with S replaced by S'. Both inequalities together yield

$$|z(S) - N\mu(S)| \leqslant N\big(c_1(A, \sigma)\Delta^{1/k}\exp\big(2(\log 2)^{1/2}k^{-1}|\log \Delta|^{1/2}\big)\big).$$

Since this holds for every $S \in \mathfrak{S}(\sigma)$, Theorem 3 is proved.

References

[1] E. Hlawka, *Discrepancy and uniform distribution of sequences*, Compositio Math. 16 (1964), pp. 83–91. (Nijenrode lecture 1962).
[2] — *Zur Definition der Diskrepanz*, Acta Arith. 18 (1971), pp. 233–241.
[3] Rudolf Mück and Walter Philipp, *Distances of probability measures and uniform distribution* mod 1, Math. Zeitschr. (to appear).
[4] F. K. Roth, *On irregularities of distribution*, Mathematika 7 (1954), pp. 73–79.
[5] W. M. Schmidt, *Irregularities of distribution. IV*, Invent. Math. 7 (1969), pp. 55–82.
[6] — *Irregularities of distribution. VII*, Acta Arith. 21 (1972), pp. 45–50.
[7] C. J. Smyth, *Inequalities relating different definitions of discrepancy*, J. Austra-lian Math. Soc. 17 (1974), pp. 81–87.
[8] — Thesis, University of Cambridge, England.
[9] S. K. Zaremba, *La discrépance isotrope et l'intégration numerique*, Ann. di Mat. pura et appl. (IV) 87 (1970), pp. 125–136.

UNIVERSITY OF COLORADO
Boulder, Colorado

Received on 6. 12. 1973 (501)

ACTA ARITHMETICA
XXVII (1975)

On power residues and exponential congruences

by

A. Schinzel (Warszawa)

In memory of Yu. V. Linnik

The main aim of this paper is to extend the results of [6] to algebraic number fields. We shall prove

Theorem 1. *Let K be an algebraic number field, ζ_q a primitive qth root of unity and τ the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$. Let $n_1, \ldots, n_k, n$ be positive integers, $n_i | n$; $\alpha_1, \ldots, \alpha_k, \beta$ be non-zero elements of K. The solubility of the k congruences $x^{n_i} \equiv \alpha_i \bmod \mathfrak{p}$ $(1 \leqslant i \leqslant k)$ implies the solubility of the congruence $x^n \equiv \beta \bmod \mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ of K if and only if at least one of the following four conditions is satisfied for suitable rational integers $l_1, \ldots, l_k, m_1, \ldots, m_k$ and suitable $\gamma, \delta \in K$:*

(i) $\beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} = \gamma^n$;

(ii) $n \not\equiv 0 \bmod 2^\tau$, $\prod_{2|n_i}\alpha_i^{l_i} = -\delta^2$ *and* $\beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} = -\gamma^n$;

(iii) $n \equiv 2^\tau \bmod 2^{\tau+1}$, $\prod_{2|n_i}\alpha_i^{l_i} = -\delta^2$ *and*

$$\beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\gamma^n;$$

(iv) $n \equiv 0 \bmod 2^{\tau+1}$ *and* $\beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\gamma^n$.

If $\zeta_4 \in K$, the conditions (ii), (iii), (iv) *imply* (i); *if $\tau = 2$,* (ii) *implies* (i) *for not necessarily the same $m_1, \ldots, m_k$ and γ.*

Almost all prime ideals means all but for a set of Dirichlet density zero or all but finitely many. In this context it comes to the same in virtue of Frobenius density theorem.

Corollary 1. *If each of the fields $K(\xi_1, \xi_2, \ldots, \xi_k)$, where $\xi_i^{n_i} = \alpha_i$ contains at least one η satisfying $\eta^n = \beta$ then at least one of the conditions* (i)–(iv) *holds.*