ACTA ARITHMETICA
XXXV (1979)

On irregularities of distribution, III

by

K. F. Roth (London)

Dedicated to Alan Fletcher

1. Introduction. Let $k>1$ and let U_0^k, U_1^k denote the unit cubes consisting respectively of points $\beta = (\beta_1, \ldots, \beta_k)$ with $0 \leqslant \beta_j < 1$ $(j = 1, \ldots, k)$ and points $\alpha = (\alpha_1, \ldots, \alpha_k)$ with $0 < \alpha_j \leqslant 1$ $(j = 1, \ldots, k)$. Let $\mathscr{P}$ be a finite set in U_0^k. For α in U_1^k, write $Z(\mathscr{P};\, \alpha)$ for the number of points of $\mathscr{P}$ lying in the box $0 \leqslant \beta_j < \alpha_j$ $(j = 1, \ldots, k)$ and put

$$D(\mathscr{P};\, \alpha) = D(\mathscr{P};\, \alpha_1, \ldots, \alpha_k) = Z(\mathscr{P};\, \alpha) - |\mathscr{P}|\alpha_1 \ldots \alpha_k,$$

where $|\mathscr{P}|$ is the number of elements of $\mathscr{P}$.

For the background of investigations regarding the function $D(\mathscr{P};\, \alpha)$, we refer the reader to [4], [2], [5].

Roth [3] proved that for every $\mathscr{P}$ in U_0^k,

$$\int_{U_1^k} |D(\mathscr{P};\, \alpha)|^2 d\alpha > c(k)\, (\log|\mathscr{P}|)^{k-1}, \tag{1.1}$$

where $c(k)$ is a positive number depending only on k.

In the case $k=2$, Davenport [1] obtained a result in the opposite direction. He made use of the existence of an irrational number θ with the property (¹) (²)

$$\nu\|\nu\theta\| > c^* > 0 \qquad (\nu = 1, 2, \ldots), \tag{1.2}$$

to construct, corresponding to every natural number M, a set $\mathscr{P}$ in U_0^2 such that $|\mathscr{P}| = 2M$ and

$$\int_0^1\int_0^1 |D(\mathscr{P};\, \xi, \eta)|^2 d\xi\, d\eta < c' \log|\mathscr{P}|. \tag{1.3}$$

(¹) $\|\alpha\|$ denotes the distance of α from a nearest integer.

(²) This property holds if and only if the continued fraction of the irrational number θ has bounded partial quotients.

This showed that (apart from the value of the constant) the inequality (1.1) is best possible in the case $k = 2$.

In the case $k = 3$, Davenport showed that the existence of a pair θ, φ with the property

$$(1.4)\qquad \nu\|\nu\theta\|\cdot\|\nu\varphi\| > c^{**} > 0 \quad (\nu = 1, 2, \ldots)$$

would enable one to construct, corresponding to each M, a set $\mathscr{P}$ in U_0^3 such that $|\mathscr{P}| = 2M$ and

$$(1.5)\qquad \int_0^1\int_0^1\int_0^1 |D(\mathscr{P};\ \xi, \eta, \zeta)|^2 d\xi\, d\eta\, d\zeta < c''(\log|\mathscr{P}|)^2.$$

The existence of a pair θ, φ with the property (1.4) is not however known, and is in fact equivalent to the falsity of a famous (open) conjecture of Littlewood.

The purpose of the present paper is to establish the existence of sets $\mathscr{P}$ in U_0^3 with the property (1.5), without the use of any unproved hypothesis. We shall prove the following result.

THEOREM 1. *For a suitable absolute constant c'' there exists, corresponding to every natural number $N \geqslant 2$, a set $\mathscr{P}$ in U_0^3 such that $|\mathscr{P}| = N$ and* (1.5) *holds.*

This establishes that the inequality (1.1) is also best possible in the case $k = 3$. We are at present (3) unable to prove analogous results for larger k.

Our method makes use of a 2-dimensional result (see § 3) which we prove by means of Davenport's technique.

The Appendix relates to our previous paper [4]. The method there can be simplified in an obvious way, after which it becomes clear that the set $\mathscr{P}_N^*$ whose existence is established in the lemma (the key result) may be taken to be simply the set consisting of the 2^s points

$$\left(\frac{t_1}{2} + \ldots + \frac{t_s}{2^s}, \frac{t_s}{2} + \ldots + \frac{t_1}{2^s}\right),$$

where each t takes, independently, the values 0 and 1. (See [4], Introduction, for a discussion of this set.)

I am indebted to Professor Niederreiter for drawing my attention(4) to the references [6], [7], and subsequently [8], concerning plane sets.

In these papers sets in U_0^2 satisfying (1.3) are constructed; these proofs, of which [8] contains the earliest, do not make use of Diophantine approximations.

(3) Since this paper was submitted, the author has succeeded in proving the analogous results for arbitrary k. The proof will appear in "On irregularities of distribution, IV", Acta Arithmetica.

(4) This acknowledgement and the relevant references added after submission of this paper.

2. Notation. We will be concerned with 3-dimensional Euclidean space, and use (x, y, z) to denote a typical point in this space. We shall also represent such a point in the vector notation

$$(2.1)\qquad \boldsymbol{v} = x\boldsymbol{i} + y\boldsymbol{j} + z\boldsymbol{k}$$

where

$$(2.2)\qquad \boldsymbol{i} = (1, 0, 0), \quad \boldsymbol{j} = (0, 1, 0), \quad \boldsymbol{k} = (0, 0, 1).$$

We use $\mathbf{0}$ for the vector $(0, 0, 0)$.

The symbol Λ is reserved for (non-degenerate) lattices in the x, y plane. Thus Λ denotes a set of the type consisting of vectors

$$(2.3)\qquad n'\boldsymbol{u}' + n''\boldsymbol{u}'',$$

where $\boldsymbol{u}', \boldsymbol{u}''$ are fixed (linearly independent) vectors of the kind $\boldsymbol{u}' = (x', y', 0)$, $\boldsymbol{u}'' = (x'', y'', 0)$ and n', n'' run independently through the integers. We use $\Lambda = \Lambda(\boldsymbol{u}', \boldsymbol{u}'')$ to express the fact that the vectors $\boldsymbol{u}', \boldsymbol{u}''$ generate Λ and write $a\Lambda$ for $\Lambda(a\boldsymbol{u}', a\boldsymbol{u}'')$.

If $\mathscr{S}$ is any subset of the (3-dimensional) space, we define (for any vector $\boldsymbol{v}^*$)

$$\boldsymbol{v}^* + \mathscr{S} = \{\boldsymbol{v}^* + \boldsymbol{v};\ \boldsymbol{v} \in \mathscr{S}\}.$$

We reserve the symbol Ω for unions of type

$$(2.4)\qquad \bigcup_{\nu=p_1}^{p_2} (\nu\boldsymbol{k} + \boldsymbol{w}_\nu + \Lambda),$$

where Λ is a lattice in the x, y plane and the $\boldsymbol{w}_\nu$ are vectors of the type

$$(2.5)\qquad \boldsymbol{w}_\nu = (x_\nu, y_\nu, 0) \quad (\nu = p_1, p_1+1, \ldots, p_2).$$

The symbol B will be reserved for boxes of type

$$(2.6)\qquad X' \leqslant x < X'', \quad Y' \leqslant y < Y'', \quad Z' \leqslant z < Z''.$$

If Ω is the set (2.4), B is the box (2.6) and $p_1 \leqslant Z' < Z'' \leqslant p_2 + 1$, we write

$$(2.7)\qquad E[\Omega;\ B] = Z(\Omega;\ B) - |d(\Lambda)|^{-1} V(B),$$

where $Z(\Omega; B)$ is the number of points of Ω in B, $d(\Lambda)$ is the determinant of the lattice Λ, and $V(B)$ is the volume of B.

An important special case is when $p_1 = p_2 = 0$, $\boldsymbol{w}_0 = \mathbf{0}$, $Z' = 0$, $Z'' = 1$. In this case $\Omega = \Lambda$ and $B = B_0(R)$ is of the form

$$(x, y) \in R, \quad 0 \leqslant z < 1,$$

where R is the rectangle

$$X' \leqslant x < X'', \quad Y' \leqslant y < Y''.$$

Accordingly, we have

$$E[\Lambda;\ B_0(R)] = Z(\Lambda;\ R) - |d(\Lambda)|^{-1}A(R),$$

where $Z(\Lambda; R)$ is the number of points of Λ in R and $A(R)$ is the area of R.

We use $\{x\}$ to denote the fractional part of x, and $\|x\|$ to denote the distance of x from a nearest integer. Thus

$$x = [x]+\{x\}, \qquad \|x\| = \min(\{x\}, 1-\{x\}).$$

3. A modification of a result of Davenport. In this section we prove a result of the same general nature as one obtained by Davenport in [1]. Only trivial modifications of Davenport's method will be required to establish this result.

Let θ be an irrational number having a continued fraction with bounded partial quotients; so that there exists a positive number $c_1 = c_1(\theta)$ such that

(3.1) $$\nu\|\nu\theta\| > c_1 \qquad (\nu = 1, 2, \ldots).$$

The number θ will remain fixed throughout, and constants implicit in the $\ll$ notation will depend only on θ.

We define the lattice Λ_0 by

(3.2) $$\Lambda_0 = \Lambda(\theta\boldsymbol{i}+\boldsymbol{j}, \boldsymbol{i}),$$

and shall retain this notation also in the subsequent section.

The result to be proved in the present section is the following. (Although the work in this section is 2-dimensional, we express our result in 3-dimensional notation for convenience of reference later.)

THEOREM A′. *Let N be a natural number and suppose that $0 < X_2'-X_1' \leqslant 1$, $0 < Y_2'-Y_1' \leqslant N$. Let B' be the box*

$$X_1' \leqslant x < X_2', \qquad Y_1' \leqslant y < Y_2', \qquad 0 \leqslant z < 1.$$

Then

(3.3) $$\int_0^1 |E[t\boldsymbol{i}+\Lambda_0;\ B']|^2\,dt \ll \log(2N).$$

We remark that, after the transformation $x\to N^{-1}x$, $y\to N^{-1}y$, the theorem may be restated in the following equivalent form.

THEOREM A″. *Let N be a natural number and suppose that $0 < X_2''-X_1'' \leqslant N^{-1}$, $0 < Y_2''-Y_1'' \leqslant 1$. Let B'' be the box*

$$X_1'' \leqslant x < X_2'', \qquad Y_1'' \leqslant y < Y_2'', \qquad 0 \leqslant z < 1.$$

Then

$$\int_0^1 |E[N^{-1}t\boldsymbol{i}+N^{-1}\Lambda_0;\ B'']|^2\,dt \ll \log(2N);$$

that is, expressed slightly differently(5)

(3.4) $$\int_0^1 |E[t\boldsymbol{i}+N^{-1}\Lambda_0;\ B'']|^2\,dt \ll \log(2N).$$

We shall require the following lemma for the proof of Theorem A′. Although the result asserted in the lemma was proved by Davenport in [1], we repeat the (short) proof here for the sake of completeness.

LEMMA A. *Let V_1 be an integer, V be a natural number, and write $e(\alpha) = \exp(2\pi i\alpha)$ (where i is the square root of -1). Then*

(3.5) $$\sum_{\nu=1}^{\infty}\frac{1}{\nu^2}\Big|\sum_{n=V_1}^{V_1+V-1} e(\theta n\nu)\Big|^2 \ll \log(2V).$$

Proof. We have

$$\Big|\sum_{n=V_1}^{V_1+V-1} e(\theta n\nu)\Big| \leqslant \min(V, \|\nu\theta\|^{-1}),$$

so that the left-hand side of (3.5) is

(3.6) $$\ll \sum_{m=1}^{\infty} 2^{-2m}\sum_{2^{m-1}\leqslant\nu<2^m}\min(V^2, \|\nu\theta\|^{-2}).$$

Now for any pair m, p of natural numbers, there are at most two values of ν in the interval $2^{m-1}\leqslant\nu<2^m$ for which

$$pc_1 2^{-m} \leqslant \|\nu\theta\| < (p+1)c_1 2^{-m};$$

for otherwise there would be two of them, say ν_1 and ν_2, whose difference $\nu_1-\nu_2$ would give a contradiction to (3.1).

Thus the expression (3.6) is

(3.7) $$\ll \sum_{m=1}^{\infty}\sum_{p=1}^{\infty}\min(2^{-2m}V^2, p^{-2}),$$

and (on splitting the outer sum into two parts corresponding to the cases $2^m \leqslant V$ and $2^m > V$) this is easily seen to be $\ll \log(2V)$ as desired.

Proof of Theorem A′. In view of the periodicity of the integrand in (3.3), we may suppose that $X_1' = 0$; we write $X_1' = 0$, $X_2' = X$ (so that $0 < X \leqslant 1$). We may also suppose that $[Y_1'] < [Y_2']$, since otherwise the result is trivial. Let B^* be the box

$$0 \leqslant x < X, \qquad [Y_1'] \leqslant y < [Y_2'], \qquad 0 \leqslant z < 1.$$

Then

$$E[t\boldsymbol{i}+\Lambda_0;\ B'] = E[t\boldsymbol{i}+\Lambda_0;\ B^*]+O(1),$$

(5) In (3.4) the range of integration is over N complete periods of the integrand.

and hence the left-hand side of (3.3) is at most $2I^*+O(1)$, where

$$I^* = \int_0^1 |E[t\boldsymbol{i}+\Lambda_0;\ B^*]|^2 dt. \tag{3.8}$$

It remains to estimate I^*. Let $\psi(x) = \{x\}-\frac{1}{2}$ when x is not an integer and $\psi(x) = 0$ when x is an integer. Then (using $0 < X \leqslant 1$),

$$\psi(x-X)-\psi(x) = \begin{cases} 1-X & \text{if } 0<\{x\}<X, \\ -X & \text{if } \{x\}>X, \end{cases}$$

and hence

$$E[t\boldsymbol{i}+\Lambda_0;\ B^*] = \sum_{n=[Y_1']}^{[Y_2']-1} \big(\psi(t+\theta n-X)-\psi(t+\theta n)\big) \tag{3.9}$$

for all but a finite number of t in the interval $0 \leqslant t < 1$.

Now $\psi(x)$ has the well known Fourier expansion

$$\psi(x) = \sum_{\nu\neq 0} -\frac{e(\nu x)}{2\pi i\nu},$$

so that the right-hand side of (3.9) has the expansion

$$\sum_{\nu\neq 0}\left(\frac{1-e(-\nu X)}{2\pi i\nu}\right)\left(\sum_{n=[Y_1']}^{[Y_2']-1} e(\theta n\nu)\right)e(\nu t).$$

It now follows from Parseval's theorem that

$$I^* \leqslant \sum_{\nu=1}^{\infty}\frac{1}{\nu^2}\left|\sum_{n=[Y_1']}^{[Y_2']-1} e(n\theta\nu)\right|^2$$

so that (3.5) yields the desired estimate for I^*.

4. The basic result. Let θ be the irrational number featuring in Section 3, and write

$$\boldsymbol{u} = \theta\boldsymbol{i}+\boldsymbol{j}, \tag{4.1}$$

so that (3.2) may be expressed in the form

$$\Lambda_0 = \Lambda(\boldsymbol{u}, \boldsymbol{i}). \tag{4.2}$$

We reserve m for non-negative integers and write

$$\Lambda_m = 2^{-m}\Lambda_0 = \Lambda(2^{-m}\boldsymbol{u}, 2^{-m}\boldsymbol{i}). \tag{4.3}$$

We define

$$\boldsymbol{q}_0 = \boldsymbol{0},\quad \boldsymbol{q}_1 = \tfrac{1}{2}\boldsymbol{u},\quad \boldsymbol{q}_2 = \tfrac{1}{2}\boldsymbol{i},\quad \boldsymbol{q}_3 = \tfrac{1}{2}\boldsymbol{u}+\tfrac{1}{2}\boldsymbol{i},$$

so that for every m,

$$\Lambda_{m+1} = \bigcup_{\tau=0}^{3}(2^{-m}\boldsymbol{q}_\tau+\Lambda_m). \tag{4.4}$$

We define $\Omega_0, \Omega_1, \ldots$ successively by

$$\Omega_0 = \Lambda_0,\qquad \Omega_{m+1} = \bigcup_{\tau=0}^{3}(\tau 4^m\boldsymbol{k}+2^{-m}\boldsymbol{q}_\tau+\Omega_m). \tag{4.5}$$

LEMMA B. *Ω_m has a representation of type (2.4) with $p_1 = 0$, $p_2 = 4^m-1$, $\Lambda = \Lambda_0$. Furthermore, the projection of Ω_m onto the x, y plane is Λ_m.*

Proof. Immediate by induction on m.

DEFINITION. We say that the box

$$0 \leqslant x < X,\quad 0 \leqslant y < Y,\quad 0 \leqslant z < Z \tag{4.6}$$

is *admissible with respect to* m if

$$0 < X \leqslant 2^{-m},\quad 0 < Y \leqslant 1,\quad 0 < Z \leqslant 4^m. \tag{4.7}$$

In the present section we establish the following basic result; and it will be shown in the next section that Theorem 1 is easily deduced from it.

THEOREM B. *There exists a number c_2, depending only on θ, such that for any m,*

$$\int_0^1\int_0^1 |E[s\boldsymbol{u}+t\boldsymbol{i}+\Omega_m;\ B]|^2 ds\, dt \leqslant c_2(m+1)^2 \tag{4.8}$$

for every box B of type (4.6) that is admissible with respect to m.

Proof. We suppose that $c_2 = c_2(\theta)$ is chosen sufficiently large. The result is trivial when $m = 0$, and we proceed by induction on m. Accordingly we suppose $m \geqslant 0$ is given and that (4.8) holds for that m for all boxes admissible with respect to m.

Suppose now we are given a box B^*, defined by

$$0 \leqslant x < X^*,\quad 0 \leqslant y < Y^*,\quad 0 \leqslant z < Z^*,$$

which is admissible with respect to $m+1$. We need to estimate

$$I = \int_0^1\int_0^1 |E[s\boldsymbol{u}+t\boldsymbol{i}+\Omega_{m+1};\ B^*]|^2 ds\, dt \tag{4.9}$$

in order to complete the induction.

Let μ be the integer determined by

$$\mu 4^m < Z^* \leqslant (\mu+1)4^m.$$

We may suppose that $0 < \mu \leqslant 3$, since in the case $\mu = 0$ the desired estimate for (4.9) is an immediate consequence of the hypothesis of induction. We write

$$B^* = \Big(\bigcup_{\tau=0}^{\mu-1} B^{(\tau)}\Big) \cup B^{**}, \tag{4.10}$$

where (for $\tau = 0, 1, 2, 3$)

(4.11) $B^{(\tau)}$ is the box $0 \leqslant x < X^*$, $0 \leqslant y < Y^*$, $\tau 4^m \leqslant z < (\tau+1)4^m$,

and

(4.12) B^{**} is the box $0 \leqslant x < X^*$, $0 \leqslant y < Y^*$, $\mu 4^m \leqslant z < Z^*$.

Now, writing

$$E_1(s,t) = \sum_{\tau=0}^{\mu-1} E[s\boldsymbol{u}+t\boldsymbol{i}+\Omega_{m+1};\ B^{(\tau)}], \tag{4.13}$$

$$E_2(s,t) = E[s\boldsymbol{u}+t\boldsymbol{i}+\Omega_{m+1};\ B^{**}], \tag{4.14}$$

we have

$$I = I_1 + I_2 + 2J, \tag{4.15}$$

where

$$I_\varkappa = \int_0^1\int_0^1 |E_\varkappa(s,t)|^2\,ds\,dt \qquad (\varkappa = 1, 2), \tag{4.16}$$

$$J = \int_0^1\int_0^1 E_1(s,t)E_2(s,t)\,ds\,dt. \tag{4.17}$$

We proceed to estimate each of I_1, I_2, J. Now

$$I_1 \leqslant \mu \sum_{\tau=0}^{\mu-1}\int_0^1\int_0^1 |E[s\boldsymbol{u}+t\boldsymbol{i}+\Omega_{m+1};\ B^{(\tau)}]|^2\,ds\,dt$$

and it follows from (4.11), (4.5) and Lemma B that

$$E[s\boldsymbol{u}+t\boldsymbol{i}+\Omega_{m+1};\ B^{(\tau)}] = E[s\boldsymbol{u}+t\boldsymbol{i}+2^{-m}\boldsymbol{q}_\tau+\Lambda_m;\ B_0], \tag{4.18}$$

where

(4.19) B_0 is the box $0 \leqslant x < X^*$, $0 \leqslant y < Y^*$, $0 \leqslant z < 1$.

Thus, in view of the periodicity (in s, t) of the expression (4.18),

$$I_1 \leqslant \mu^2 M, \tag{4.20}$$

where

$$M = \int_0^1\int_0^1 |E[s\boldsymbol{u}+t\boldsymbol{i}+\Lambda_m;\ B_0]|^2\,ds\,dt. \tag{4.21}$$

Furthermore, since B^* is admissible with respect to $m+1$ (so that $0 < X^* \leqslant 2^{-m-1} < 2^{-m}$, $0 < Y^* \leqslant 1$), it follows from Theorem A″ of the previous section (with $N = 2^m$) that

$$M \ll m+1. \tag{4.22}$$

By (4.5), (4.12) (and the definition of μ),

$$E_2(s,t) = E[s\boldsymbol{u}+t\boldsymbol{i}+2^{-m}\boldsymbol{q}_\mu+\Omega_m;\ -\mu 4^m\boldsymbol{k}+B^{**}].$$

Furthermore, this expression is periodic with period 1 in each of s and t, so that

$$I_2 = \int_0^1\int_0^1 |E[s\boldsymbol{u}+t\boldsymbol{i}+\Omega_m;\ -\mu 4^m\boldsymbol{k}+B^{**}]|^2\,ds\,dt.$$

The box $-\mu 4^m\boldsymbol{k}+B^{**}$ is admissible with respect to m, and hence

$$I_2 \leqslant c_2(m+1)^2. \tag{4.23}$$

It remains to estimate J. The integrand in (4.17) is periodic with period 1 in each of s and t, and hence

$$J = \int_0^1\int_0^1 E_1(s+a2^{-m}, t+b2^{-m})E_2(s+a2^{-m}, t+b2^{-m})\,ds\,dt$$

for every a, b. But it follows from (4.13) and the relations (4.18) that $E_1(s,t)$ is in fact periodic with period 2^{-m} in each of s and t. Thus

$$4^m J = \int_0^1\int_0^1 E_1(s,t)D(s,t)\,ds\,dt, \tag{4.24}$$

where

$$D(s,t) = \sum_{a=0}^{2^m-1}\sum_{b=0}^{2^m-1} E_2(s+a2^{-m}, t+b2^{-m}). \tag{4.25}$$

In view of (4.16), (4.20), (4.22), we have by Schwarz's inequality,

$$(4^m J)^2 \ll (m+1)\int_0^1\int_0^1 |D(s,t)|^2\,ds\,dt. \tag{4.26}$$

Now from (4.14) and (4.25) it follows that (with the meanings of Z and V as in (2.7))

$$D(s,t) = Z(s\boldsymbol{u}+t\boldsymbol{i}+\Omega';\ B^{**}) - 4^m V(B^{**}), \tag{4.27}$$

where

$$\Omega' = \bigcup_{a=0}^{2^m-1}\bigcup_{b=0}^{2^m-1}(a2^{-m}\boldsymbol{u}+b2^{-m}\boldsymbol{i}+\Omega_{m+1}).$$

We note that B^{**} is contained in the box $B^{(\mu)}$ (see (4.11), (4.12)). In view of (4.5), we may therefore replace Ω' in (4.27) by

$$\mu 4^m \boldsymbol{k} + 2^{-m}\boldsymbol{q}_\mu + \Omega'', \tag{4.28}$$

where

$$\Omega'' = \bigcup_{a=0}^{2^m-1}\bigcup_{b=0}^{2^m-1}(a2^{-m}\boldsymbol{u}+b2^{-m}\boldsymbol{i}+\Omega_m).$$

It is clear from the first assertion of Lemma B that Ω'' has a representation

$$\Omega'' = \bigcup_{\nu=0}^{4^m-1}(\nu\boldsymbol{k}+\boldsymbol{w}_\nu+\Lambda_m)$$

(with $\boldsymbol{w}_\nu$ in the x, y plane), and it then follows from the second assertion of Lemma B that in fact

$$\Omega'' = \bigcup_{\nu=0}^{4^m-1}(\nu\boldsymbol{k}+\Lambda_m).$$

We slightly modify the box B^{**} (see (4.12)) by replacing Z^* by the least integer greater than or equal to Z^*. This leaves the first term on the right-hand side of (4.27) unchanged, and introduces an error of at most 2^m in the second term. Thus, writing

$$h_1 = \mu 4^m, \quad h_2 = -[-Z^*],$$

and using (4.27) with Ω' replaced by (4.28), we have

$$D(s,t) = (h_2-h_1)E[2^{-m}\boldsymbol{q}_\mu+s\boldsymbol{u}+t\boldsymbol{i}+\Lambda_m;\ B_0]+O(2^m),$$

where B_0 is defined by (4.19). Thus

$$\int_0^1\int_0^1 |D(s,t)|^2\,ds\,dt \ll 4^{2m}(M+1),$$

where M is the integral (4.21), so that in view of (4.22), (4.26),

$$J \ll m+1. \tag{4.29}$$

Since c_2 is sufficiently large, we obtain $I \leqslant c_2(m+2)^2$ on using our estimates for I_1, I_2, J (see (4.20), (4.22), (4.23), (4.29)) in (4.15). This establishes the estimate for (4.9) required to complete the induction.

5. Deduction of Theorem 1. Let the natural number $N \geqslant 2$ be given and choose m to satisfy $2^{m-1} < N \leqslant 2^m$. For this m, take $B = B(X, Y, Z)$ to be the box (4.6) and integrate (4.8) with respect to X, Y, Z over the region K given by

$$0 < X \leqslant 2^{-m}, \quad 0 < Y \leqslant N2^{-m}, \quad 0 < Z \leqslant 4^m.$$

It follows from the resulting inequality that there exist s^*, t^* (satisfying

$0 \leqslant s^* < 1$, $0 \leqslant t^* < 1$) such that

$$\iiint_K |E[s^*\boldsymbol{u}+t^*\boldsymbol{i}+\Omega_m;\ B(X,Y,Z)]|^2\,dX\,dY\,dZ \leqslant c_2(m+1)^2N. \tag{5.1}$$

It follows from Lemma B that there are exactly N points of $s^*\boldsymbol{u}+t^*\boldsymbol{i}+\Omega_m$ in the region

$$0 \leqslant x < 2^{-m}, \quad 0 \leqslant y < N2^{-m}, \quad 0 \leqslant z < 4^m.$$

Let these be the points

$$(2^{-m}x_\nu^*,\ N2^{-m}y_\nu^*,\ 4^m z_\nu^*) \quad (\nu = 0, 1, \ldots, N-1)$$

and let $\mathscr{P}$ consist of the N points

$$(x_\nu^*, y_\nu^*, z_\nu^*) \quad (\nu = 0, 1, \ldots, N-1).$$

Then $\mathscr{P}$ is certainly contained in the cube U_0^3, and on making the substitutions $X = 2^{-m}\xi$, $Y = N2^{-m}\eta$, $Z = 4^m\zeta$ in (5.1), we obtain the desired inequality of type (1.5).

Appendix

The purpose of this appendix is to describe an obvious simplification of the lemma in [4].

In the inductive proof of that lemma, we proceeded from a set $\mathscr{P}_N^*$ (already constructed) to sets

$$\mathscr{P}_{2N}^{(a)} \quad (a = 0, 1, \ldots, N-1).$$

After estimating the average value of the expression (2.13) over $a = 0, 1, \ldots$ $\ldots, N-1$, we deduced that for at least one such a the set $\mathscr{P}_{2N}^{(a)}$ has the property required to complete the induction.

However, on noting that the first term on the right-hand side of (2.7) has period N^{-1} in t, it becomes clear that the value of

$$\int_0^1 |E[\mathscr{P}_{2N}^{(a)}(t);\ x, y]|^2\,dt$$

is in fact independent of a. It follows that the expression (2.13) is independent of a, so that we may take $a = 0$ at each step of the induction. The resulting set (2.1) consists simply of the first 2^s terms of the well known van der Corput sequence, magnified by a factor 2^s.

References

[1] H. Davenport, *Note on irregularities of distribution*, Mathematika 3 (1956), pp. 131–135.

[2] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience, 1974, Chapter 2.

[3] K. F. Roth, *On irregularities of distribution*, Mathematika 1 (1954), pp. 73–79.
[4] — *On irregularities of distribution, II*, Communications on Pure and Applied Math. XXIX (1976), pp. 749–754.
[5] Wolfgang M. Schmidt, *Irregularities of distribution, X*, Journal of Number Theory, to appear.
[6] J. H. Halton and S. K. Zaremba, *The extreme and L^2 discrepancies of some plane sets*, Monatsh. für Math. 73 (1969), pp. 316–328.
[7] Brian E. White, *Mean-square discrepancies of the Hammersley and Zaremba sequences for arbitrary radix*, ibid. 80 (1975), pp. 219–229.
[8] I. V. Vilenkin, *Plane nets of integration* (Russian), Ž. Vyčisl. Mat. i Mat. Fiz. 7 (1967), pp. 189–196; Engl. transl. in U.S.S.R. Comp. Math. and Math. Phys. 7 (1) (1967), pp. 258–267.

IMPERIAL COLLEGE
London S. W. 7, England

Received on 11. 1. 1977 (908)

ACTA ARITHMETICA
XXXV (1979)

Dihedral extensions of Q of degree $2l$ which contain non-Galois extensions with class number not divisible by l

by

KIYOAKI IIMURA (Tokyo)

1. Main results. In this paper we specify all dihedral extensions K of degree $2l$ over the rational numbers Q which contain non-Galois extensions of odd prime degree $l \neq 3$ over Q with class number not divisible by l in terms of the conductor of the cyclic extension K/k of degree l, where k is a unique quadratic subfield of K. In [3] F. Gerth III completely gave the discriminants of all (non-Galois) cubic extensions of Q whose class numbers are not divisible by 3. Our paper extends in essence his work to all non-Galois extensions of Q of odd prime degree $l \neq 3$ whose normal closures have degree $2l$ over Q.

Now to state our results we need the following fact proved by J. Martinet [7].

LEMMA 1. *Let K be a dihedral extension of Q of degree $2l$, where l is an odd prime number $\neq 3$, let k be the quadratic subfield of K with discriminant d, and let L be a non-Galois extension of Q of degree l contained in K. Then the conductor f of the cyclic extension K/k of degree l has the following form:*

$$f = l^{u+v} \prod_i p_i \prod_j q_j,$$

where p_i and q_j are rational primes such that

$$p_i \equiv \left(\frac{d}{p_i}\right) = 1 \pmod{l},$$

$$q_j \equiv \left(\frac{d}{q_j}\right) = -1 \pmod{l};$$

$u = 1$ if $l \mid f$ and $l \nmid d$, $u = 0$ otherwise; and $v = 0$ or 1.

Furthermore the discriminant of L/Q is $d^{(l-1)/2} f^{l-1}$.

Our main result is: