Mathematical Journal of Okayama University

Volume 18, *Issue* 1 1975 *Article* 2

DECEMBER 1975

Uniform distribution of sequences of algebraic integers

H. Niederreiter* Siu Kwong Lo†

*University Of California

†Benedict College

UNIFORM DISTRIBUTION OF SEQUENCES OF ALGEBRAIC INTEGERS

H. NIEDERREITER*) and SIU KWONG LO

1. Introduction and summary. The definition of the uniform distribution of sequences of algebraic integers in a fixed algebraic number field K was first introduced by Kuipers, Niederreiter, and Shiue [4]. The concept contains as special cases the notion of uniform distribution of sequences of Gaussian integers studied in [4] and the notion of uniform distribution of sequences of rational integers introduced by Niven [10]. In the present paper, we shall establish some important general facts concerning uniformly distributed sequences of algebraic integers in K. The measure-theoretic and density-theoretic aspects of this notion of uniform distribution were studied in [9].

In Section 2, we prove various forms of the Weyl criterion for uniform distribution of sequences of algebraic integers in K, based either on an ideal-theoretic or on a module-theoretic viewpoint. In Section 3, we discuss the connection between the uniform distribution of sequences of algebraic integers in K and of sequences of integers in the various localizations of K. A certain subring of the adèle ring of K is constructed as a suitable compactification of the additive group of algebraic integers in K and is used to establish a number of important properties of uniformly distributed sequences of algebraic integers in K. In Section 4, interesting results about the relation between the uniform distribution of sequences of algebraic integers and of sequences of rational integers are obtained.

2. Weyl criterion. Let K be a given algebraic number field of degree k over the field $\mathbf{Q}$ of rationals, and let O be the ring of algebraic integers in K. Let I be a nontrivial integral ideal in O with counting norm $\mathcal{N}I$. If $\mathscr{A}=(\alpha_n)$, $n=1, 2, \cdots$, is a sequence of elements in O, then we use $A(N, \alpha+I, \mathscr{A})$ to denote the number of n, $1\leq n\leq N$, such that $\alpha_n\equiv\alpha \pmod I$. The following two definitions can be found in [4].

Definition 2.1. Let $I\subset O$ be a nontrivial integral ideal. Then the sequence $\mathscr{A}$ is uniformly distributed modulo I (u. d. mod I) if

*) The research of the first author was supported by NSF Grant MPS 72—05055 A02.

Mathematical Journal of Okayama University, Vol. 18 [1975], Iss. 1, Art. 2

$$\lim_{N\to\infty} \frac{A(N, \alpha+I, \mathscr{A})}{N} = \frac{1}{\mathscr{N} I}$$

for every coset $\alpha+I$ of I.

Definition 2.2. The sequence $\mathscr{A}$ is uniformly distributed in O (u. d. in O) if $\mathscr{A}$ is u. d. mod I for every nontrivial integral ideal $I\subset O$.

Remark. Uniformly distributed sequences in O have been constructed in [9].

Let $W=\{\omega_1, \cdots, \omega_k\}$ be an integral basis for K over $\mathbf{Q}$. Then every $\alpha\in O$ can be uniquely expressed in the form $\alpha=\sum_{i=1}^{k} x_i\omega_i$, where each x_i is in $\mathbf{Z}$, the ring of rational integers. If one identifies α with the lattice point $x=(x_1, \cdots, x_k)$ in $\mathbf{Z}^k$, the set of all k-dimensional lattice points, then O can be identified with $\mathbf{Z}^k$. It turns out that, at least as far as the additive structure is concerned, the discussion of uniform distribution of sequences in O is equivalent to the discussion of uniform distribution of sequences in $\mathbf{Z}^k$ (see [9, Section 2]). For the latter theory, see [6] and [7]. Because of this equivalence, the definition of uniform distribution of sequences in O can be viewed as a special case of a definition of Rubel [11].

We shall write $\exp(a)=e^{2\pi i a}$ for any real number a. The general criterion for uniform distribution of sequences in $\mathbf{Z}^k$ is known to be the Weyl criterion [7, Theorem 2. 2] which, when translated into a criterion for uniform distribution in O, reads as follows.

Theorem 2.3. (Weyl criterion). *Let* $W=\{\omega_1, \cdots, \omega_k\}$ *be an integral basis for* K *over* $\mathbf{Q}$. *Then the sequence* $\mathscr{A}=(\alpha_n)$, $n=1, 2, \cdots$, *with* $\alpha_n=x_{n1}\omega_1+\cdots+x_{nk}\omega_k$ *for* $n\geqq 1$, *where* $x_{nj}\in\mathbf{Z}$ *for* $n\geqq 1$ *and* $j=1, \cdots, k$, *is u. d. in* O *if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp(a_1x_{n1}+\cdots+a_kx_{nk})=0$$

for all k-tuples $(a_1, \cdots, a_k)$ *of rationals, not all* a_i *being rational integers.*

It is desirable to have criteria for the uniform distribution modulo a single integral ideal I. The following theorem ([2], see also [3, p. 227]) establishes a foundation for the subsequent discussion in this section.

Theorem 2.4. (Eckmann). *Let H be a compact abelian group and $\hat{H}$ its character group. A sequence (h_n), $n=1, 2, \cdots$, is u.d. in H if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi(h_n)=0$$

for each nontrivial $\chi\in\hat{H}$.

For each nontrivial integral ideal I, we will view O/I as a compact additive group in the discrete topology. We shall be searching for explicit forms of the characters of O/I.

Let J be a fractional ideal in K. Then J^* is defined by

$$J^*=\{\alpha\in K:\ \mathrm{Tr}_{K/\mathbf{Q}}(\alpha J)\subseteq\mathbf{Z}\},$$

where $\mathrm{Tr}_{K/\mathbf{Q}}: K\longrightarrow\mathbf{Q}$ is the trace function from K to $\mathbf{Q}$. J^* is called the complementary set of J. We note that $J^*=O^*J^{-1}$, $(J^*)^{-1}$ is called the different of J, and $(O^*)^{-1}$ is the different of the field K (see [12, p. 155]).

$\mathscr{P}$ will denote a prime ideal in O, P its corresponding prime divisor, and ν_P will be the normalized exponential valuation belonging to P. As a matter of convenience, we shall often define a character of O/I as a mapping on O. Of course, we have to verify that the mapping on O depends on the residue classes mod I only.

Theorem 2.5. *Let $I\subset O$ be a nontrivial integral ideal. Then the characters of O/I are given by*

$$\chi_\beta(\alpha)=\exp\left(\mathrm{Tr}_{K/\mathbf{Q}}(\alpha\beta)\right)\ \text{for}\ \alpha\in O,$$

where β runs through a complete system of representatives of I^*/O^*.

Proof. It is evident that χ_β is a homomorphism from O to the circle group. Let α be in I. Since $\beta\in I^*$, we have $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha\beta)\in\mathbf{Z}$, which implies that $\chi_\beta(\alpha)=1$, i.e., χ_β is trivial on I. Thus, χ_β can be viewed as a character of O/I.

We claim that if $\beta_1, \beta_2\in I^*$ with $\beta_1-\beta_2\notin O^*$, then $\chi_{\beta_1}\neq\chi_{\beta_2}$. Indeed, there is an $\alpha\in O$ such that $\mathrm{Tr}_{K/\mathbf{Q}}((\beta_1-\beta_2)\alpha)\notin\mathbf{Z}$. So, $\chi_{\beta_1}(\alpha)\neq\chi_{\beta_2}(\alpha)$.

Since distinct representatives of I^*/O^* give distinct characters and the group of characters of O/I is isomorphic to O/I, the proof will be complete once we show that the cardinality of I^*/O^* is $\mathscr{N}I$. Let $\{\delta_1, \cdots, \delta_{\mathscr{N}I}\}$ be a complete system of representatives of O/I. Let

$$I=\prod_{i=1}^{m}\mathscr{P}_i^{t_i} \quad \text{and} \quad O^*=\prod_{i=1}^{m}\mathscr{P}_i^{a_i}.$$

Then

$$I^*/O^*=\prod_{i=1}^{m}\mathscr{P}_i^{a_i-t_i}\Big/\prod_{i=1}^{m}\mathscr{P}_i^{a_i}.$$

By the Strong Approximation Theorem [12, p. 123], there is a $\gamma\in K$ such that $\nu_{P_i}(\gamma)=a_i-t_i$ for $i=1,\cdots,m$, and $\nu_P(\gamma)\geq 0$ for $P\neq P_1,\cdots,P_m$. Now one checks in a straightforward way that $\{\gamma\delta_1,\cdots,\gamma\delta_{\mathscr{N}I}\}$ forms a complete system of representatives for I^*/O^*, and so we are done.

Corollary 2.6. *The sequence $\mathscr{A}=(\alpha_n)$, $n=1,2,\cdots$, in O is u.d.* mod I *if and only if*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\exp(\mathrm{Tr}_{K/Q}(\alpha_n\beta))=0$$

for all $\beta\in I^*$ with $\beta\notin O^*$.

If $W=\{\omega_1,\cdots,\omega_k\}$ is an integral basis for K over $\mathbf{Q}$, then every nontrivial integral ideal I possesses a canonical basis $\{\nu_1,\cdots,\nu_k\}$ of the form

$$\begin{aligned}
\nu_1&=h_{11}\omega_1+\cdots+h_{1k}\omega_k\\
\nu_2&=h_{22}\omega_2+\cdots+h_{2k}\omega_k\\
&\vdots \qquad\qquad\qquad \vdots\\
\nu_k&=\qquad\qquad\quad h_{kk}\omega_k
\end{aligned}$$

such that $\prod_{i=1}^{k}h_{ii}=\mathscr{N}I$ and I is a $\mathbf{Z}$-module with basis $\{\nu_1,\cdots,\nu_k\}$ (see [12, p. 163]).

If $\boldsymbol{a}=(a_1,\cdots,a_k)$ and $\boldsymbol{b}=(b_1,\cdots,b_k)$ are two vectors of the Euclidean space $\mathbf{R}^k$, then $\boldsymbol{a}\cdot\boldsymbol{b}=\sum_{i=1}^{k}a_ib_i$ denotes their standard inner product. In the following, we give an alternative formula for the characters of O/I.

Theorem 2.7. *Suppose I is an integral ideal with canonical basis $\{\nu_1,\cdots,\nu_k\}$, $\nu_i=\sum_{j=i}^{k}h_{ij}\omega_j$ for $i=1,\cdots,k$, and m is a positive rational integer such that $mO\subseteq I$. Then the characters of O/I are given by*

$$\chi^{(j)}(\alpha)=\exp\left(\left(\frac{j_1}{m},\cdots,\frac{j_k}{m}\right)\cdot(x_1,\cdots,x_k)\right),$$

where $\alpha=x_1\omega_1+\cdots+x_k\omega_k\in O$ and the k-tuple $\boldsymbol{j}=(j_1,\cdots,j_k)$ of rational integers satisfies the following conditions:

(1) $(j_1, \cdots, j_k)$ *is a solution of the system*

$$\begin{aligned} j_1h_{11}+j_2h_{12}+\cdots+j_kh_{1k}&\equiv 0 \pmod m\\ j_2h_{22}+\cdots+j_kh_{2k}&\equiv 0 \pmod m\\ &\vdots\\ j_kh_{kk}&\equiv 0 \pmod m\end{aligned}$$

(2) $0\leq j_i<m$ for $i=1, \cdots, k$.

Proof. From character theory, we know that the characters of O/mO are given by

$$\chi^{(j)}(\alpha)=\exp\left(\left(\frac{j_1}{m}, \cdots, \frac{j_k}{m}\right)\cdot(x_1, \cdots, x_k)\right),$$

where $j=(j_1, \cdots, j_k)$ with $0\leq j_i<m$ for $i=1, \cdots, k$, and that the characters of O/I are those $\chi^{(j)}$ which are trivial on I/mO.

It is evident that a character of O/mO is trivial on I/mO if and only if it is trivial on ν_i+mO for $1\leq i\leq k$. Thus, in order to find all characters of O/I, one needs to find all $\chi^{(j)}$ such that $\chi^{(j)}(\nu_i)=1$ for $1\leqq i\leqq k$ simultaneously. Equivalently, one needs to find all k-tuples $j=(j_1, \cdots, j_k)$, $0\leq j_i<m$ for $i=1, \cdots, k$, such that

$$\begin{aligned} j_1h_{11}+j_2h_{12}+\cdots+j_kh_{1k}&\equiv 0 \pmod m\\ j_2h_{22}+\cdots+j_kh_{2k}&\equiv 0 \pmod m\\ &\vdots\\ j_kh_{kk}&\equiv 0 \pmod m\end{aligned}$$

Remark. It is suggested to use $\mathscr{N}I$ for m in the preceding theorem, in view of the fact that the coset identity $(\mathscr{N}I)(1+I)=I$ implies $\mathscr{N}I\in I$.

In certain special cases, other types of character formulas can be given.

Definition 2.8. Let K be an algebraic number field with integral basis $\{\omega_1, \cdots, \omega_k\}$. Then for every element $\alpha=x_1\omega_1+\cdots+x_k\omega_k$ in K, we define the projection map L_i, $i=1, \cdots, k$, by $L_i(\alpha)=x_i$.

Theorem 2.9. *If* $K=\mathbf{Q}(\alpha)$ *with integral basis* $\{1, \alpha, \cdots, \alpha^{k-1}\}$ *and* $\theta\neq 0$ *is an algebraic integer in* K, *then the characters of the additive group* $O/\theta O$ *are given by*

$$\chi_\beta(\delta)=\exp\left(L_k(\beta\delta/\theta)\right),$$

where β *and* δ *are algebraic integers in* K.

Proof. It is obvious that χ_β is a group homomorphism from O to the circle group. We shall show that $\chi_\beta(\delta)$ depends only on the residue class of δ mod θO. If $\delta_1 \equiv \delta_2 \pmod{\theta O}$, then $\beta(\delta_1-\delta_2)/\theta = x_1 + x_2\alpha + \cdots + x_k\alpha^{k-1}$ with $x_i \in \mathbf{Z}$, $i=1, \cdots, k$. So, $L_k(\beta(\delta_1-\delta_2)/\theta) = x_k$. Hence,

$$\frac{\chi_\beta(\delta_1)}{\chi_\beta(\delta_2)} = \exp(x_k) = 1.$$

We claim that if $\beta_1 \not\equiv \beta_2 \pmod{\theta O}$, then $\chi_{\beta_1} \neq \chi_{\beta_2}$. Indeed, $(\beta_1-\beta_2)/\theta = a_1 + a_2\alpha + \cdots + a_k\alpha^{k-1}$ and at least one of the $a_i \in \mathbf{Q}\backslash\mathbf{Z}$. Let m be the largest index such that $a_m \in \mathbf{Q}\backslash\mathbf{Z}$. Then $a_j \in \mathbf{Z}$ for $m < j \leqq k$. Consider

$$(*) \quad \frac{\beta_1-\beta_2}{\theta}\alpha^{k-m} = a_1\alpha^{k-m} + a_2\alpha^{k-m+1} + \cdots + a_m\alpha^{k-1} + a_{m+1}\alpha^k + \cdots + a_k\alpha^{2k-m-1}.$$

Since $a_{m+1}\alpha^k + \cdots + a_k\alpha^{2k-m-1}$ is an algebraic integer, the total coefficient b of α^{k-1} in (*) is in $\mathbf{Q}\backslash\mathbf{Z}$, i. e.,

$$b = L_k\left(\frac{\beta_1-\beta_2}{\theta}\alpha^{k-m}\right) \in \mathbf{Q}\backslash\mathbf{Z}.$$

Thus, $\chi_{\beta_1}(\alpha^{k-m}) \neq \chi_{\beta_2}(\alpha^{k-m})$. Therefore, we have found all characters, since there are as many as $\mathcal{N}(\theta O)$ which are all distinct.

Remark. Theorem 2. 9 provides a convenient method to find the characters of $O/\theta O$. This theorem applies to many algebraic number fields, for instance, the quadratic fields. For necessary and sufficient conditions for $\mathbf{Q}(\alpha)$ to possess the integral basis $\{1, \alpha, \cdots, \alpha^{k-1}\}$, the reader is referred to [12, p. 164].

If O/I is cyclic, then O/I is generated by $1+I$ (see Theorem 4. 2). Let $\varphi : O \longmapsto O/I$ be the natural homomorphism and $\psi : O/I \longmapsto \{0, \cdots, \mathcal{N}I-1\}$ such that $\psi(r+I) = r$ for $r = 0, \cdots, \mathcal{N}I-1$. The characters of O/I are given by

$$\chi_j(\alpha) = \exp\left(\frac{j(\psi \circ \varphi)(\alpha)}{\mathcal{N}I}\right) \quad \text{for } \alpha \in O,$$

where $j = 0, \cdots, \mathcal{N}I-1$. The reader is referred to Theorem 4. 4 for the characterization of O/I to be cyclic.

Based on the character formula for finite fields [5, p. 90], the following assertion is evident. Let $\mathcal{P}$ be a prime ideal of O with $\mathcal{N}\mathcal{P} = p^f$ and let φ be the natural homomorphism from O to $O/\mathcal{P}$. We write $\varphi(\alpha) = \bar{\alpha}$. Then the characters of $O/\mathcal{P}$ are given by

$$\chi_{\bar{\alpha}}(\bar{\beta}) = \exp\left(\frac{1}{p}\sum_{i=0}^{f-1}(\bar{\alpha}\bar{\beta})^{p^i}\right) \quad \text{for } \bar{\beta} \in O/\mathcal{P},$$

where $\bar{\alpha} \in O/\mathscr{P}$.

We shall give a simple application of the results established so far. The following theorem was shown in [13].

Theorem 2.10. (Zame). *Let G be a locally compact abelian group with countable base. Also, let $\mathscr{S} \neq \Phi$, $\mathscr{T}$ be countable collections of closed subgroups of G such that:*

(i) *finite intersections of elements of $\mathscr{S} \cup \mathscr{T}$ are of compact index;*

(ii) *for each $S \in \mathscr{S}$ and $T \in \mathscr{T}$, we have $S \not\supseteq T$;*

(iii) *for each $T \in \mathscr{T}$, there exists a character χ_T of G such that χ_T is trivial on T but is nontrivial on each $S \in \mathscr{S}$.*

Then there is a sequence (g_n), $n=1, 2, \cdots$, in G such that (g_n) is u.d. mod *S for all $S \in \mathscr{S}$, but not u.d.* mod *T for $T \in \mathscr{T}$.*

Theorem 2.11. *Let $\{I_m\}$* and *$\{J_n\}$ be countable collections of nontrivial ideals in O such that $I_m \not\subseteq J_n$ for $m, n = 1, 2, \cdots$* and *J_n^* is principal for $n=1, 2, \cdots$. Then there exists a sequence in O which is u.d.* mod *I_m for $m=1, 2, \cdots$, but which, for $n=1, 2, \cdots$, is not u.d.* mod *J_n.*

Proof. We put $\mathscr{S} = \{I_m\}$, $m=1, 2, \cdots$, and $\mathscr{T} = \{J_n\}$, $n=1, 2, \cdots$, in Theorem 2.10. It suffices to check condition (iii) of that theorem. Take a fixed J_n. Since J_n^* is principal, we have $J_n^* = \gamma O$ for some $\gamma \in J_n^*$. Then the character $\chi_\gamma(\alpha) = \exp(\mathrm{Tr}_{K/Q}(\alpha\gamma))$, $\alpha \in O$, is trivial on J_n. Suppose χ_γ were trivial on some I_m. It follows that $\gamma \in I_m^*$. Thus, $J_n^* = \gamma O \subseteq I_m^*$, which implies $I_m \subseteq J_n$, a contradiction.

Corollary 2.12. *If $K = \mathbf{Q}(\alpha)$ has the integral basis $\{1, \alpha, \cdots, \alpha^{k-1}\}$ and $\{I_m\}$, $\{\theta_n O\}$ are countable collections of nontrivial integral ideals with $I_m \quad \theta_n O$ for $m, n=1, 2, \cdots$, then there is a sequence in O that is u.d.* mod *I_m for $m=1, 2, \cdots$, but which, for $n=1, 2, \cdots$, is not u.d.* mod *$\theta_n O$.*

Proof. Let f be the minimal polynomial of α over $\mathbf{Q}$. Then $O^* = (f'(\alpha))^{-1} O$ (see [12, p. 164]). Thus, $(\theta_n O)^* = (\theta_n f'(\alpha))^{-1} O$, which is principal for $n=1, 2, \cdots$. The rest follows from Theorem 2.11.

Theorem 2.13. *There exists a sequence in O that is u.d. modulo all powers of all prime ideals, but not u.d. in O.*

Proof. In Theorem 2.11, we take $\{I_m\}$ to be an enumeration of all powers of all prime ideals. Let $O^* = \prod_{i=1}^{s} \mathscr{P}_i^{-r_i}$ with $r_i > 0$ for $1 \leqq i \leqq s$

($s=0$ if $k=1$). Let h be the class number of K, and let $\mathscr{Q}_1 \neq \mathscr{Q}_2$ be two prime ideals that are both distinct from $\mathscr{P}_1, \cdots, \mathscr{P}_s$. Put

$$J=\mathscr{Q}_1^h \mathscr{Q}_2^h \prod_{i=1}^{s} \mathscr{P}_i^{(h-1)r_i}.$$

We note that $I_m \subsetneq J$ for $m=1, 2, \cdots$ since J is not a power of a prime ideal, and that $J^*=J^{-1}O^*=(\mathscr{Q}_1^{-1}\mathscr{Q}_2^{-1}O^*)^h$, which is principal as the h-th power of a fractional ideal. Let $\{J\}$ play the role of the second collection of ideals in Theorem 2. 11, and the proof is complete.

3. Global and local uniform distribution. We shall use K_P to denote the local completion of an algebraic number field K at the non-trivial discrete prime divisor P. Let O_P be the ring of integers in K_P and $\tau \in O$ such that $\nu_P(\tau)=1$. The fundamental neighborhoods of zero in K_P are given by $\tau^t O_P$ with $t \in \mathbf{Z}$. They are simultaneously closed and open. K_P is a second countable locally compact group with respect to addition and O_P is a compact subgroup of K_P. Every $\delta \in K_P$ has a unique expansion $\delta=\sum_{i=r}^{\infty} \alpha_i \tau^i$, $r \in \mathbf{Z}$, with $\alpha_r \neq 0$ for $\delta \neq 0$ and $\alpha_i \in \mathscr{R}$ for $i \geq r$, where $\mathscr{R}$ is a fixed complete system of representatives of $O/\mathscr{P}$ (see [12, p. 35]).

Since O_P is a compact group, the definition of uniform distribution is conventionally given with respect to the Haar measure (see [3, Chapter 4]). However, we find that the following equivalent definition is more convenient. The proof of the equivalence is essentially the same as the proof of Lemma 3. 6.

Definition 3.1. Let $\Delta=(\delta_n)$, $n=1, 2, \cdots$, be a sequence of elements of O_P. Then Δ is u. d. in O_P if Δ is u. d. mod $\tau^t O_P$ (in the obvious sense) for all positive integers t.

Theorem 3.2. *Let $\mathscr{A}=(\alpha_n)$, $n=1, 2, \cdots$, be a sequence of algebraic integers in O. Then for every $t \geq 1$, $\mathscr{A}$ is u. d.* mod $\mathscr{P}^t$ *if and only if $\mathscr{A}$ is u. d.* mod $\tau^t O_P$.

Proof. For $\alpha, \beta \in O$, we have $\alpha \equiv \beta \pmod{\tau^t O_P}$ if and only if $\nu_P(\alpha-\beta) \geq t$ if and only if $\alpha \equiv \beta \pmod{\mathscr{P}^t}$. Hence, $A(N, \beta+\mathscr{P}^t, \mathscr{A})=A(N, \beta+\tau^t O_P, \mathscr{A})$. So,

$$\lim_{N\to\infty} \frac{A(N, \beta+\mathscr{P}^t, \mathscr{A})}{N} = \lim_{N\to\infty} \frac{A(N, \beta+\tau^t O_P, \mathscr{A})}{N}$$

whenever one of the two limits exists; thus, $\mathscr{A}$ is u. d. mod $\mathscr{P}^t$ if and only if $\mathscr{A}$ is u. d. mod $\tau^t O_P$.

The following two corollaries are immediate consequences.

Corollary 3.3. *If $\mathscr{A}=(\alpha_n)$, $n=1,2,\cdots$, is a sequence of algebraic integers in O, then $\mathscr{A}$ is u.d. in O_P if and only if $\mathscr{A}$ is u.d.* mod $\mathscr{P}^t$ *for all $t\geq 1$.*

Corollary 3.4. *If $\mathscr{A}=(\alpha_n)$, $n=1,2,\cdots$, is a u.d. sequence in O, then $\mathscr{A}$ is u.d. in O_P for all nontrivial discrete prime divisors P.*

Let $\delta=\sum_{i=r}^{\infty}\alpha_i\tau^i$ be in O_P. We set $S_m(\delta)=\sum_{i=r}^{m}\alpha_i\tau^i$ for $m\geq r$ and $S_m(\delta)=0$ for $m<r$.

Theorem 3.5. *Let $\Delta=(\delta_n)$, $n=1,2,\cdots$, be a sequence of elements of O_P. Then Δ is u.d. in O_P if and only if for each $m=0,1,\cdots$, the sequence $(S_m(\delta_n))$, $n=1,2,\cdots$, is u.d.* mod $\mathscr{P}^{m+1}$ *in O.*

Proof. Let $\delta_n=\sum_{i=0}^{\infty}\alpha_{ni}\tau^i$ for $n=1,2,\cdots$. Since $\delta_n-S_m(\delta_n)=\sum_{i=m+1}^{\infty}\alpha_{ni}\tau^i\in\tau^{m+1}O_P$, the sequence Δ is u.d. mod $\tau^{m+1}O_P$ if and only if $(S_m(\delta_n))$, $n=1,2,\cdots$, is u.d. mod $\mathscr{P}^{m+1}$ in O. Consequently, Δ is u.d. in O_P if and only if $(S_m(\delta_n))$, $n=1,2,\cdots$, is u.d. mod $\mathscr{P}^{m+1}$ in O for $m=0,1,\cdots$.

Let $\mathscr{O}$ denote the Cartesian product $\mathscr{O}=\times_P O_P$, where P runs through the set of all nontrivial discrete prime divisors of K. Let $\mathscr{O}$ be furnished with the product topology. Then $\mathscr{O}$ is a second countable compact group with respect to coordinatewise addition. $\mathscr{O}$ can also be viewed as a subring of the adèle ring of K. Let μ be the Haar measure on $\mathscr{O}$. Then a μ-u.d. sequence in $\mathscr{O}$ is simply said to be u.d. in $\mathscr{O}$ (see [3, Chapter 4]).

For the remainder of this section, we shall assume, unless otherwise specified, that all the prime ideals in O have been enumerated in some fixed way, say $\mathscr{P}_1,\mathscr{P}_2,\cdots$. For $j\geq 1$, let $\tau_j\in O$ such that $\nu_{P_j}(\tau_j)=1$. By a fundamental neighborhood in $\mathscr{O}$, we mean a set $V\subseteq\mathscr{O}$ of the form $V=\times_{j=1}^{\infty}V_j$, where $V_j=O_{P_j}$ for all but finitely many j and V_j is a coset of $\tau_j^{t_j}O_{P_j}$, $t_j\geq 1$, for those $V_j\neq O_{P_j}$.

Lemma 3.6. *A sequence $\Gamma=(\gamma_n)$, $n=1,2,\cdots$, is u.d. in $\mathscr{O}$ if and only if*

$$\lim_{N\to\infty}\frac{A(N,V,\Gamma)}{N}=\mu(V)$$

holds for every fundamental neighborhood V in $\mathscr{O}$, where $A(N,V,\Gamma)$ is the number of n, $1\leq n\leq N$, with $\gamma_n\in V$.

Proof. Evidently, a fundamental neighborhood V in $\mathcal{O}$ is simultaneously closed and open. Thus, V is a μ-continuity set and the necessity of the condition follows from [3, Chapter 3, Theorem 1.2].

To prove sufficiency, let $\mathcal{M}$ be the collection of all fundamental neighborhoods in $\mathcal{O}$, together with the empty set. Let $E\neq\emptyset$ be an open set in $\mathcal{O}$. By the regularity of μ, for any $\varepsilon>0$ there exists a closed set $C\subseteq E$ with $\mu(E\backslash C)<\varepsilon$. Let $\{V_\iota\}$, $V_\iota\subseteq E$, be an open cover for C consisting of fundamental neighborhoods. By the compactness of C, there exists a finite subcover $\{V_1, \cdots, V_r\}$. Then $\mu(E\backslash\bigcup_{j=1}^{r} V_j)<\varepsilon$. By [3, Chapter 3, Exercise 1.15], the collection of characteristic functions of elements in $\mathcal{M}$ forms a convergence-determining class [3, p. 172] with respect to μ. So, the sufficiency is proved.

Let $i_P: O\longmapsto O_P$ be the canonical embedding. Then $i=\bigtimes_P i_P$: $O\longmapsto\mathcal{O}$ is an injective homomorphism which maps O into the "diagonal" of $\mathcal{O}$. For the purpose of simplicity, when $\alpha\in O$, we shall use the symbol α to denote α, $i_P(\alpha)$, and $i(\alpha)$. The meaning will be clear from the context.

We note that every nonzero ideal in O can be expressed in the form $I=\prod_{j=1}^{r}\mathscr{P}_j^{s_j}$ with $s_j\geq 0$ for $j=1, \cdots, r$.

Lemma 3.7. *Let $\alpha\in O$ and let $\beta+I$ be a coset of the nonzero integral ideal $I=\prod_{j=1}^{r}\mathscr{P}_j^{s_j}$. Then $\alpha\in\beta+I$ if and only if α is in the fundamental neighborhood $V=\bigtimes_{j=1}^{\infty}V_j$ in $\mathcal{O}$ with $V_j=\beta_j+\tau_j^{s_j}O_{P_j}$ for $j=1, \cdots, r$ and $V_j=O_{P_j}$ for $j>r$, where $\beta_j\in O$ and $\beta_j\equiv\beta \pmod{\mathscr{P}_j^{s_j}}$ for $j=1, \cdots, r$.*

Proof. $\alpha\in\beta+I$ is equivalent to $\alpha-\beta\in\mathscr{P}_j^{s_j}$ for $j=1, \cdots, r$, which, in turn, is equivalent to $\alpha-\beta_j\in\mathscr{P}_j^{s_j}$ for $j=1, \cdots, r$. The latter condition holds if and only if $\alpha-\beta_j\in\tau_j^{s_j}O_{P_j}$ for $j=1, \cdots, r$, and this is satisfied precisely if $\alpha\in V$.

Theorem 3.8. *Let $\mathscr{A}=(\alpha_n)$, $n=1, 2, \cdots$, be a sequence of elements of O. Then $\mathscr{A}$ is u. d. in O if and only if $\mathscr{A}$ is u. d. in $\mathcal{O}$.*

Proof. Suppose $\mathscr{A}$ is u. d. in $\mathcal{O}$. Let $\beta+I$ be a coset of the nontrivial integral ideal I and V be the fundamental neighborhood in $\mathcal{O}$ constructed in Lemma 3.7. Then, $A(N, \beta+I, \mathscr{A})=A(N, V, \mathscr{A})$, and so

$$\lim_{N\to\infty}\frac{A(N, \beta+I, \mathscr{A})}{N}=\lim_{N\to\infty}\frac{A(N, V, \mathscr{A})}{N}=\mu(V)=\frac{1}{\mathscr{N}I}$$

by Lemma 3. 6. Thus, $\mathscr{A}$ is u. d. in O.

Conversely, suppose $\mathscr{A}$ is u. d. in O. Let V be a fundamental neighborhood in $\mathscr{O}$, say $V=\bigtimes_{j=1}^{\infty} V_j$ with $V_j=\beta_j+\tau_j^{s_j}O_{P_j}$ for $j=1, \cdots, r$ and $V_j=O_{P_j}$ for $j>r$, where $\beta_j\in O$ for $j=1, \cdots, r$. By the Chinese Remainder Theorem, there exists a $\beta\in O$ with $\beta_j\equiv\beta \pmod{\mathscr{P}_j^{s_j}}$ for $j=1, \cdots, r$. Then, with $I=\prod_{j=1}^{r}\mathscr{P}_j^{s_j}$, we have $A(N,V,\mathscr{A})=A(N,\beta+I,\mathscr{A})$ according to Lemma 3. 7. It follows that

$$\lim_{N\to\infty}\frac{A(N, V, \mathscr{A})}{N}=\lim_{N\to\infty}\frac{A(N, \beta+I, \mathscr{A})}{N}=\frac{1}{\mathscr{N}I}=\mu(V),$$

and so $\mathscr{A}$ is u. d. in $\mathscr{O}$ by Lemma 3. 6.

Remark. According to a terminology introduced by Berg, Rajagopalan, and Rubel [1], one may call $\mathscr{O}$ the D-compactification of O.

Let $\mathscr{B}$ be the algebra generated by the empty set and the cosets of nonzero ideals of O. A finitely additive measure ν called the Banach-Buck measure (see [9, Section 4]) can be defined on $\mathscr{B}$. Let ν^* be the outer measure which extends ν. In [9, Theorem 4. 5] it was proved that a set $A\subseteq O$ satisfies $\nu^*(A)=1$ if and only if A intersects every coset of every nonzero integral ideal.

Theorem 3.9. *Let $A\subseteq O$. Then the elements of A can be arranged into a u. d. sequence in O if and only if $\nu^*(A)=1$.*

Proof. If the elements of A can be arranged into a u. d. sequence in O, then $\nu^*(A)=1$ by [9, Theorem 4. 8].

Conversely, suppose $\nu^*(A)=1$. Then, by the remark preceding Theorem 3. 9, A intersects every coset of every nonzero integral ideal. By Lemma 3. 7 and the Chinese Remainder Theorem, A is dense in $\mathscr{O}$. By [3, Chapter 3, Theorem 2. 5] (see also [8] for more general results), the elements of A can be arranged into a u. d. sequence in $\mathscr{O}$. An application of Theorem 3. 8 completes the proof.

Corollary 3.10. *The set C of all composite algebraic integers in O can be arranged into a u. d. sequence in O.*

Proof. In [9, Example 4. 6] it was shown that $\nu^*(C)=1$. Thus, the corollary follows from Theorem 3. 9.

Remark. For $O=\mathbf{Z}$, the result of the above corollary was shown by Niven [10].

Based on the methods of this section, we give an alternative proof of Theorem 2. 13 for the case when $[K:\mathbf{Q}]\geq 2$. The case $K=\mathbf{Q}$ was proved by Niven [10]. We shall construct a normed regular Borel measure μ_1 on $\mathscr{O}$ which is different from the Haar measure μ but has the same projections as μ has on each coordinate space O_P. Since O is dense in $\mathscr{O}$, it can be arranged into a μ_1-u. d. sequence $\mathscr{A}$. However, μ_1 is different from μ, and so $\mathscr{A}$ is not u. d. in O. Since μ and μ_1 have the same projection on each O_P, $\mathscr{A}$ is u. d. in each O_P. By Corollary 3. 3, this means that $\mathscr{A}$ is u. d. modulo all powers of all prime ideals in O.

For the sake of brevity, we only sketch the construction of μ_1. By choosing two prime ideals in O that lie over a rational prime splitting completely in K, we obtain prime ideals $\mathscr{P}_1$ and $\mathscr{P}_2$ with $\mathscr{N}\mathscr{P}_1=\mathscr{N}\mathscr{P}_2=q$, say. By a square of degree r in $O_{P_1}\times O_{P_2}$ we mean a Cartesian product of cosets of the form $(\alpha+\tau_1^r O_{P_1})\times(\beta+\tau_2^r O_{P_2})$, $\alpha\in O_{P_1}$, $\beta\in O_{P_2}$, r a positive rational integer. We label the distinct cosets of $\tau_1 O_{P_1}$ by $\alpha_{11}+\tau_1 O_{P_1},\cdots,\alpha_{q1}+\tau_1 O_{P_1}$ and the distinct cosets of $\tau_2 O_{P_2}$ by $\beta_{11}+\tau_2 O_{P_2},\cdots,\beta_{q1}+\tau_2 O_{P_2}$. Then $(\alpha_{i1}+\tau_1 O_{P_1})\times(\beta_{j1}+\tau_2 O_{P_2})$ is called a diagonal square of degree 1 if $i=j$. Each one of the q diagonal squares of degree 1 contains q diagonal squares of degree 2 obtained in an analogous fashion. Similarly, we can construct the diagonal squares of degree m which are inside the diagonal squares of degree $m-1$. Let $\mathscr{C}$ be the algebra generated by all the squares in $O_{P_1}\times O_{P_2}$. Define a set function φ_1' from the generators of $\mathscr{C}$ to the nonnegative reals by

$$\varphi_1'((\alpha+\tau_1^n O_{P_1})\times(\beta+\tau_2^n O_{P_2}))=q^{-n}$$

if $(\alpha+\tau_1^n O_{P_1})\times(\beta+\tau_2^n O_{P_2})$ is a diagonal square of degree n and

$$\varphi_1'((\alpha+\tau_1^n O_{P_1})\times(\beta+\tau_2^n O_{P_2}))=0 \text{ otherwise.}$$

It can be proved that φ_1' can be extended uniquely to a normed regular Borel measure φ_1 on $O_{P_1}\times O_{P_2}$. Evidently, φ_1 is distinct from the Haar measure on $O_{P_1}\times O_{P_2}$, but has the same projections on O_{P_i} for $i=1,2$ as the Haar measure. We let φ_2 be the Haar measure on $\bigtimes_{i=3}^{\infty} O_{P_i}$ and set $\mu_1=\varphi_1\times\varphi_2$. Then μ_1 is the desired measure.

4. Uniform distribution of algebraic integers and of rational integers. Since the uniform distribution in $\mathbf{Z}^k$ and in O are equivalent (see [9, Section 2]), these two concepts will be used interchangeably in this section. The following theorem was first proved in [7, Theorem 2. 3] for $\mathbf{Z}^k$.

Theorem 4.1. (Niederreiter). *Let K be an algebraic number field with integral basis $\{\omega_1, \cdots, \omega_k\}$ over* $\mathbf{Q}$ *and let $\mathscr{A}=(\alpha_n)$, $n=1, 2, \cdots$, with $\alpha_n=x_{n1}\omega_1+\cdots+x_{nk}\omega_k$ for $n\geq 1$, be a sequence in O. The sequence $\mathscr{A}$ is u.d. in O if and only if for all k-tuples $(s_1, \cdots, s_k)$ of rational integers with* g.c.d. $(s_1, \cdots, s_k)=1$, *the sequences (σ_n), $n=1, 2, \cdots$, with $\sigma_n=s_1x_{n1}+\cdots+s_kx_{nk}$ for $n\geq 1$, are* u.d. *in* $\mathbf{Z}$.

In the discussion to follow later on, one will find that the uniform distribution of a sequence in O modulo a single ideal I is equivalent to the uniform distribution mod $\mathscr{N}I$ of a certain sequence in $\mathbf{Z}$ whenever O/I is cyclic. Here we give the characterization of O/I to be cyclic.

Theorem 4.2. *Let K be an algebraic number field with integral basis $\{\omega_1, \cdots, \omega_k\}$ over* $\mathbf{Q}$, *let I be a nontrivial integral ideal, and let m be the smallest positive rational integer in I. The following statements are equivalent*:

(1) *O/I is cyclic*;

(2) *there is a sequence $X=(x_n)$, $n=1, 2, \cdots$, of rational integers and an $\alpha\in O$ such that $(x_n\alpha)$, $n=1, 2, \cdots$, is u.d.* mod I;

(3) $m=\mathscr{N}I$;

(4) *there is a sequence $Y=(y_n)$, $n=1, 2, \cdots$, of rational integers such that Y is u.d.* mod I;

(5) $\omega_i\equiv d_i \pmod{I}$ *for some $d_i\in\mathbf{Z}$, for $i=1, \cdots, k$.*

Proof. Assume (1). Then O/I is generated by $\alpha+I$ for some $\alpha\in O$. Choose $X=(n\alpha)$, $n=1, 2, \cdots$. Then (2) follows.

Assume (2). Then $\alpha+I$ is a generator of O/I. Since $m\in I$, we have $m\alpha\equiv 0 \pmod{I}$, and so $\mathscr{N}I$ divides m. On the other hand, $m\leq\mathscr{N}I$, and (3) follows.

Assume (3). Then $1+I$ is a generator of O/I. Choose $Y=(n)$, $n=1, 2, \cdots$, then (4) is true.

Assume (4). Then each residue class mod I contains a rational integer, and (5) follows.

Assume (5). Then each coset of I is of the form $d+I$ for some $d\in\mathbf{Z}$, and (1) follows.

Theorem 4.3. *Let $\mathscr{P}$ be a prime ideal in O with ramification index e and residue class degree f over* $\mathbf{Q}$.

(1) *When $e=1$, $O/\mathscr{P}^t$ is cyclic if and only if $f=1$. In this case, t can be an arbitrary positive rational integer.*

(2) *When $e>1$, $O/\mathscr{P}^t$ is cyclic if and only if $f=t=1$.*

Proof. If a is a real number, we use $\langle a\rangle$ to denote the smallest rational integer $\geq a$. Suppose $\mathscr{P}$ lies over the rational prime p. Let n be a positive integer such that $n\in\mathscr{P}^t$. This is equivalent to $\nu_p(n)\geq t/e$. Thus the smallest positive rational integer m in $\mathscr{P}^t$ is $m=p^{\langle t/e\rangle}$. By Theorem 4.2, $O/\mathscr{P}^t$ is cyclic if and only if $tf=\langle t/e\rangle$ (since $\mathscr{N}\mathscr{P}^t=p^{tf}$). We consider the equation $tf=\langle t/e\rangle$ with the unknown t being a positive rational integer.

Case 1: when $e=1$, the equation has a solution if and only if $f=1$. In this case, t is arbitrary.

Case 2: $e>1$. If $t\leq e$, then $tf=\langle t/e\rangle$ has a solution if and only if $f=t=1$. If $t>e$, then $tf=\langle t/e\rangle$ has no solution since $\langle t/e\rangle<t/e+1<t\leq tf$.

Theorem 4.4. *Suppose* $I=\prod_{i=1}^{r}\mathscr{P}_i^{t_i}$, *where the* $\mathscr{P}_i$ *are distinct prime ideals with ramification indices* e_i, $1\leq i\leq r$, *and residue class degrees* f_i, $1\leq i\leq r$, *and where* $t_i\geq 1$ *for* $1\leq i\leq r$. *Then* O/I *is cyclic if and only if* g. c. d. $(\mathscr{N}\mathscr{P}_i,\mathscr{N}\mathscr{P}_j)=1$ *for* $i\neq j$, $f_i=1$ *for* $1\leq i\leq r$, *and* $t_i=1$ *whenever* $e_i>1$.

Proof. By the Chinese Remainder Theorem, we have $O/I\cong\bigoplus_{i=1}^{r}(O/\mathscr{P}_i^{t_i})$. Thus, the sufficiency is a direct consequence of Theorem 4.3 and of g. c. d. $(\mathscr{N}\mathscr{P}_i^{t_i},\mathscr{N}\mathscr{P}_j^{t_j})=1$ for $i\neq j$.

As for the necessity, one notices first that $O/\mathscr{P}_i^{t_i}$ is cyclic for $i=1,\cdots,r$. Thus, by Theorem 4.3, $f_i=1$ for $1\leq i\leq r$ and $t_i=1$ whenever $e_i>1$. Without loss of generality, suppose $\mathscr{N}\mathscr{P}_1=p^{f_1}$ and $\mathscr{N}\mathscr{P}_2=p^{f_2}$. Since $O/I\cong(O/\mathscr{P}_1^{t_1}\mathscr{P}_2^{t_2})\oplus(O/\prod_{i=3}^{r}\mathscr{P}_i^{t_i})$, it suffices to show that $O/\mathscr{P}_1^{t_1}\mathscr{P}_2^{t_2}$ is not cyclic to arrive at a contradiction. For a real number a, let $\langle a\rangle$ be the smallest rational integer $\geq a$. A positive rational integer n is in $\mathscr{P}_1^{t_1}\mathscr{P}_2^{t_2}$ if and only if $\nu_p(n)\geq t_1/e_1$ and $\nu_p(n)\geq t_2/e_2$. Hence, the smallest positive rational integer m in $\mathscr{P}_1^{t_1}\mathscr{P}_2^{t_2}$ is $m=\max_{i=1,2}p^{\langle t_i/e_i\rangle}$. By Theorem 4.2, $O/\mathscr{P}_1^{t_1}\mathscr{P}_2^{t_2}$ is cyclic if and only if $\max_{i=1,2}\langle t_i/e_i\rangle=f_1t_1+f_2t_2$. However, it is obvious that $\max_{i=1,2}\langle t_i/e_i\rangle<f_1t_1+f_2t_2$, and this yields the desired contradiction.

Theorem 4.5. *Let* K *be an algebraic number field with integral basis* $\{\omega_1,\cdots,\omega_k\}$ *over* $\mathbf{Q}$, *and let* I *be a nontrivial integral ideal. Suppose* $\omega_i\equiv d_i$ (mod I) *for* $1\leq i\leq k$, *where* $d_i\in\mathbf{Z}$ *for* $1\leq i\leq k$. *Then a sequence* $\mathscr{A}=(\alpha_n)$, $n=1,2,\cdots$, *in* O *with* $\alpha_n=x_{n1}\omega_1+\cdots+x_{nk}\omega_k$ *for* $n\geq 1$ *is u. d.* mod I *if and only if the sequence* (σ_n), $n=1,2,\cdots$, *with* $\sigma_n=x_{n1}d_1+\cdots+x_{nk}d_k$ *for* $n\geq 1$, *is u. d.* mod $\mathscr{N}I$ *in* $\mathbf{Z}$.

Proof. Since $\sigma_n \equiv \alpha_n \pmod I$, the sequence $\mathscr{A}$ can be replaced mod I by the sequence (σ_n), $n=1,2,\cdots$. According to Theorem 4.2, $\{0, 1, \cdots, \mathscr{N}I-1\}$ constitutes a complete system of representatives of O/I, and if $d \in \mathbf{Z}$, we have

$$A(N, d+I, (\sigma_n)) = A(N, d+(\mathscr{N}I)\mathbf{Z}, (\sigma_n)),$$

since $a \equiv b \pmod I$ is equivalent to $a \equiv b \pmod{\mathscr{N}I}$ for $a, b \in \mathbf{Z}$. Thus, the theorem follows.

Corollary 4.6. *Suppose $K=\mathbf{Q}(\alpha)$ with integral basis $\{1, \alpha, \cdots, \alpha^{k-1}\}$ over $\mathbf{Q}$ and I is a nontrivial integral ideal with $\alpha \equiv d \pmod I$ for some $d \in \mathbf{Z}$. Then a sequence $\mathscr{A}=(\alpha_n)$, $n=1,2,\cdots$, in O with $\alpha_n = x_{n0} + x_{n1}\alpha + \cdots + x_{n,k-1}\alpha^{k-1}$ for $n \geq 1$ is u.d. mod I if and only if the sequence (σ_n), $n=1,2,\cdots$, where $\sigma_n = x_{n0} + x_{n1}d + \cdots + x_{n,k-1}d^{k-1}$ for $n \geq 1$, is u.d. mod $\mathscr{N}I$ in $\mathbf{Z}$.*

Theorem 4.7. *Suppose $\mathscr{A}=(\alpha_n)$, $n=1,2,\cdots$, is u.d. in O. Then there exists a natural number m, independent of $\mathscr{A}$, such that the sequence $\left(\frac{1}{m}\operatorname{Tr}_{K/\mathbf{Q}}(\alpha_n)\right)$, $n=1,2,\cdots$, is u.d. in $\mathbf{Z}$.*

Proof. It is obvious that $\operatorname{Tr}_{K/\mathbf{Q}} : O \longrightarrow \mathbf{Z}$ is an additive group homomorphism. Thus, there is a natural number m such that $\operatorname{Tr}_{K/\mathbf{Q}}(O) = m\mathbf{Z}$. Since the topologies on O and $\mathbf{Z}$ are discrete, $\frac{1}{m}\operatorname{Tr}_{K/\mathbf{Q}}$ is an open, onto, continuous homomorphism. By [3, Chapter 4, Theorem 5.1], we know that $\left(\frac{1}{m}\operatorname{Tr}_{K/\mathbf{Q}}(\alpha_n)\right)$, $n=1,2,\cdots$, is u.d. in $\mathbf{Z}$.

Theorem 4.8. *Let $(m_1, \cdots, m_k) \in \mathbf{Z}^k$ with $m_i \geq 1$ for $1 \leq i \leq k$, and let $X=(\mathbf{x}_n)$, $n=1,2,\cdots$, with $\mathbf{x}_n = (x_{n1}, \cdots, x_{nk})$ for $n \geq 1$, be a sequence of lattice points. Then X is u.d. mod $(m_1, \cdots, m_k)$ in $\mathbf{Z}^k$ if and only if the sequences (σ_n), $n=1,2,\cdots$, with*

$$\sigma_n = \frac{1}{m}(j_1 m_2 \cdots m_k x_{n1} + \cdots + j_k m_1 \cdots m_{k-1} x_{nk}) \quad \text{for} \quad n \geq 1,$$

are u.d. mod $\left(\frac{1}{m}\prod_{i=1}^{k} m_i\right)$ in $\mathbf{Z}$ for any k-tuple $(j_1, \cdots, j_k) \neq (0, \cdots, 0)$ in $\mathbf{Z}^k$ with $0 \leq j_i < m_i$ for $1 \leq i \leq k$ and $m = \text{g.c.d.}\left(\prod_{i=1}^{k} m_i, j_1 m_2 \cdots m_k, \cdots, j_k m_1 \cdots m_{k-1}\right)$.

Proof. To prove necessity, let $t \in \mathbf{Z}$ with $1 \leq t < \frac{1}{m}\prod_{i=1}^{k} m_i$ and set

$$\frac{t}{\frac{1}{m}\prod_{i=1}^{k} m_i}=\frac{p}{q}, \quad \text{where g. c. d. } (p, q)=1 \text{ and } q\geq 1.$$

Obviously, $q>1$. Put

$$s_1=\frac{j_1m_2\cdots m_k}{m}, \cdots, s_k=\frac{j_km_1\cdots m_{k-1}}{m}.$$

We claim that at least one of the $\frac{p}{q}s_i$ is not an integer. For otherwise, $q|s_i$ for $1\leq i\leq k$ and $q|\frac{1}{m}\prod_{i=1}^{k} m_i$, which implies that qm is a common divisor of $\prod_{i=1}^{k} m_i$, $j_1m_2\cdots m_k, \cdots, j_km_1\cdots m_{k-1}$. But $qm>m$, yielding a contradiction. Thus, by [7, Theorem 2.1], one has

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\exp\left(\frac{t}{\frac{1}{m}\prod_{i=1}^{k} m_i}(s_1x_{n1}+\cdots+s_kx_{nk})\right)$$
$$=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\exp\left(\frac{tj_1}{m_1}x_{n1}+\cdots+\frac{tj_k}{m_k}x_{nk}\right)=0,$$

and the desired conclusion follows from [3, Chapter 5, Theorem 1.2].

To prove sufficiency, let $(j_1, \cdots, j_k)$ be as in the theorem. Then,

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\exp\left(\frac{j_1}{m_1}x_{n1}+\cdots+\frac{j_k}{m_k}x_{nk}\right)$$
$$=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\exp\left(\frac{1}{\frac{1}{m}\prod_{i=1}^{k} m_i}(s_1x_{n1}+\cdots+s_kx_{nk})\right)=0$$

by [3, Chapter 5, Theorem 1.2], and the desired conclusion follows from [7, Theorem 2.1].

As an immediate consequence of the above theorem, we obtain the following result.

Corollary 4.9. *Let K be an algebraic number field with integral basis $\{\omega_1, \cdots, \omega_k\}$ over* $\mathbf{Q}$. *If $I=m_1\omega_1\mathbf{Z}\oplus\cdots\oplus m_k\omega_k\mathbf{Z}$, $m_i\in\mathbf{Z}$, $m_i\geq 1$ for $i=1, \cdots, k$, is a nontrivial integral ideal and $\mathscr{A}=(\alpha_n)$, $n=1, 2, \cdots$, with $\alpha_n=x_{n1}\omega_1+\cdots+x_{nk}\omega_k$ for $n\geq 1$, is a sequence of algebraic integers, then $\mathscr{A}$ is u. d.* mod I *if and only if the sequences (σ_n), $n=1, 2, \cdots$, with*

$$\sigma_n=\frac{1}{m}(j_1m_2\cdots m_kx_{n1}+\cdots+j_km_1\cdots m_{k-1}x_{nk}) \quad for \quad n\geq 1,$$

are u.d. $\operatorname{mod}\left(\frac{\mathcal{N}I}{m}\right)$ *in* $\mathbf{Z}$ *for every k-tuple* $(j_1, \cdots, j_k) \neq (0, \cdots, 0)$ *in* $\mathbf{Z}^k$ *with* $0 \leq j_i < m_i$ *for* $1 \leq i \leq k$ *and* $m = \text{g. c. d.}(\mathcal{N}I, j_1 m_2 \cdots m_k, \cdots, j_k m_1 \cdots m_{k-1})$.

REFERENCES

[1] I. D. BERG, M. RAJAGOPALAN, and L. A. RUBEL: Uniform distribution in locally compact abelian groups, Trans. Amer. Math. Soc. **133** (1968), 435—446.

[2] B. ECKMANN: Über monothetische Gruppen, Comment. Math. Helv. **16** (1943/44), 249—263.

[3] L. KUIPERS and H. NIEDERREITER: Uniform Distribution of Sequences, Wiley-Interscience, New York, 1974.

[4] L. KUIPERS, H. NIEDERREITER, and J.-S. SHIUE: Uniform distribution of sequences in the ring of Gaussian integers, Bull. Inst. Math. Acad. Sinica, to appear.

[5] S. LANG: Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.

[6] H. NIEDERREITER: Uniform distribution of lattice points, Proc. Number Theory Conf. (Boulder, Colo., 1972), pp. 162—166.

[7] ______________: On a class of sequences of lattice points, J. Number Th. **4** (1972), 477—502.

[8] ______________: Rearrangement theorems for sequences, Journées Arithmétiques de Bordeaux 1974, Collection Astérisque, Vol. **24—25**, pp. 243—261, Soc. Math. France, Paris, 1975.

[9] H. NIEDERREITER and S. K. LO: Banach-Buck measure, density, and uniform distribution in rings of algebraic integers, Pacific J. Math., to appear.

[10] I. NIVEN: Uniform distribution of sequences of integers, Trans. Amer. Math. Soc. **98** (1961), 52—61.

[11] L. A. RUBEL: Uniform distribution in locally compact groups, Comment. Math. Helv. **39** (1965), 253—258.

[12] E. WEISS: Algebraic Number Theory, McGraw-Hill, New York, 1963.

[13] A. ZAME: On a problem of Narkiewicz concerning uniform distributions of sequences of integers, Colloq. Math. **24** (1972), 271—273.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA
LOS ANGELES, CA 90024
U. S. A.

DEPARTMENT OF MATHEMATICS
BENEDICT COLLEGE
COLUMBIA, S. C. 29204
U. S. A.

(*Received December 4, 1974*)