Uniform distribution of sequences of algebraic integers

H. Niederreiter*  Siu Kwong Lo†
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 $\mathbb{Q}$ 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 $M^{|I|}$. If $\mathcal{X}=(\alpha_n)$, $n=1, 2, \ldots$, is a sequence of elements in $O$, then we use $A(N, \alpha+I, \mathcal{X})$ 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 $\mathcal{X}$ 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.
for every coset $\alpha + I$ of $I$.

**Definition 2.2.** The sequence $\mathcal{S}$ is uniformly distributed in $O$ (u.d. in $O$) if $\mathcal{S}$ 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 $\mathbb{Q}$. 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 $\mathbb{Z}$, the ring of rational integers. If one identifies $\alpha$ with the lattice point $x = (x_1, \cdots, x_k)$ in $\mathbb{Z}^k$, the set of all $k$-dimensional lattice points, then $O$ can be identified with $\mathbb{Z}^k$. 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 $\mathbb{Z}^k$ (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 $\exp (a) = e^{a \alpha}$ for any real number $a$. The general criterion for uniform distribution of sequences in $\mathbb{Z}^k$ 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 $\mathbb{Q}$. Then the sequence $\mathcal{S} = (\alpha_n)$, $n = 1, 2, \cdots$, with $\alpha_n = x_{n_1} \omega_1 + \cdots + x_{n_k} \omega_k$ for $n \geq 1$, where $x_{n_j} \in \mathbb{Z}$ for $n \geq 1$ and $j = 1, \cdots, k$, is u.d. in $O$ if and only if $\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \exp \left( a_1 x_{n_1} + \cdots + a_k x_{n_k} \right) = 0$

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

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

where $\text{Tr}_{K/Q} : K \to \mathbb{Q}$ is the trace function from $K$ to $\mathbb{Q}$. $J^*$ 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]).

$\mathcal{P}$ will denote a prime ideal in $O$, $P$ its corresponding prime divisor, and $r_p$ 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 $I \subseteq O$ be a nontrivial integral ideal. Then the characters of $O/I$ are given by

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

where $\beta$ runs through a complete system of representatives of $I^*/O^*$.

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

We claim that if $\beta_1, \beta_2 \in I^*$ with $\beta_1 - \beta_2 \not\in O^*$, then $\chi_{\beta_1} \neq \chi_{\beta_2}$. Indeed, there is an $\alpha \in O$ such that $\text{Tr}_{K/Q}(\beta_1 - \beta_2) \alpha \not\in \mathbb{Z}$. 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 $\mathcal{V}(I)$. Let $\{ \beta_1, \cdots, \beta_m \}$ be a complete system of representatives of $O/I$. Let
H. NIEDERREITER and S. K. LO

\[ I = \prod_{i=1}^{m} \mathcal{Q}_i^{a_i} \quad \text{and} \quad O^* = \prod_{i=1}^{m} \mathcal{Q}_i^{b_i}. \]

Then

\[ I^*/O^* = \prod_{i=1}^{m} \mathcal{Q}_i^{a_i-b_i}. \]

By the Strong Approximation Theorem [12, p. 123], there is a \( r \in K \) such that \( \nu_p(r) = a_i - b_i \), for \( i = 1, \ldots, m \), and \( \nu_p(r) \geq 0 \) for \( P \neq P_1, \ldots, P_m \).

Now one checks in a straightforward way that \( \{ r \delta_1, \ldots, r \delta_m \} \) forms a complete system of representatives for \( I^*/O^* \), and so we are done.

**Corollary 2.6.** The sequence \( \mathcal{A} = (\alpha_n) \), \( n = 1, 2, \ldots \), in \( O \) is univalent modulo \( I \) if and only if

\[ \lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \exp \left( \text{Tr}_{K/Q}(\alpha_n \beta) \right) = 0 \]

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

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

\begin{align*}
\nu_1 &= h_{11} \omega_1 + \cdots + h_{1k} \omega_k \\
\nu_2 &= h_{21} \omega_1 + \cdots + h_{2k} \omega_k \\
&\vdots \\
\nu_k &= h_{k1} \omega_1 + \cdots + h_{kk} \omega_k
\end{align*}

such that \( \prod_{i=1}^{k} h_{ii} = \mathcal{A}^{-1} I \) and \( I \) is a \( \mathbb{Z} \)-module with basis \( \{ \nu_1, \ldots, \nu_k \} \) (see [12, p. 163]).

If \( a = (a_1, \ldots, a_k) \) and \( b = (b_1, \ldots, b_k) \) are two vectors of the Euclidean space \( \mathbb{R}^k \), then \( a \cdot b = \sum_{i=1}^{k} a_i b_i \) 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 \( \{ \nu_1, \ldots, \nu_k \} \), \( \nu_i = \sum_{j=1}^{k} h_{ij} \omega_j \), for \( i = 1, \ldots, k \), and \( m \) is a positive rational integer such that \( mO \subseteq I \). Then the characters of \( O/I \) are given by

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

where \( \alpha = x_1 \omega_1 + \cdots + x_k \omega_k \in O \) and the \( k \)-tuple \( j = (j_1, \ldots, j_k) \) of rational integers satisfies the following conditions:
UNIFORM DISTRIBUTION OF ALGEBRAIC INTEGERS

(1) \((j_1, \ldots, j_k)\) is a solution of the system

\[
\begin{align*}
j_1h_{11} + j_2h_{12} + \cdots + j_kh_{1k} &\equiv 0 \pmod{m} \\
j_2h_{21} + \cdots + j_kh_{2k} &\equiv 0 \pmod{m} \\
&\vdots \\
j_kh_{kk} &\equiv 0 \pmod{m}
\end{align*}
\]

(2) \(0 \leq j_i \leq m\) for \(i = 1, \ldots, k\).

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

\[
\chi^{(J)}(\alpha) = \exp \left( \left( \frac{j_1}{m}, \ldots, \frac{j_k}{m} \right) \cdot (x_1, \ldots, x_k) \right),
\]

where \(j = (j_1, \ldots, j_k)\) with \(0 \leq j_i \leq m\) for \(i = 1, \ldots, k\), 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 \(\nu_i + mO\) 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 \(1 \leq i \leq k\) simultaneously. Equivalently, one needs to find all \(k\)-tuples \(j = (j_1, \ldots, j_k)\), \(0 \leq j_i \leq m\) for \(i = 1, \ldots, k\), such that

\[
\begin{align*}
j_1h_{11} + j_2h_{12} + \cdots + j_kh_{1k} &\equiv 0 \pmod{m} \\
j_2h_{21} + \cdots + j_kh_{2k} &\equiv 0 \pmod{m} \\
&\vdots \\
j_kh_{kk} &\equiv 0 \pmod{m}
\end{align*}
\]

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

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 \(\{\omega_1, \ldots, \omega_k\}\). Then for every element \(\alpha = x_1\omega_1 + \cdots + x_k\omega_k \in K\), we define the projection map \(L_i\), \(i = 1, \ldots, k\), by \(L_i(\alpha) = x_i\).

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

\[
\chi(\beta) = \exp \left( L_i(\beta \delta / \theta) \right),
\]

where \(\beta\) and \(\delta\) are algebraic integers in \(K\).
Proof. It is obvious that $\chi_{\varphi}$ is a group homomorphism from $O$ to the circle group. We shall show that $\chi_{\varphi}(\alpha)$ depends only on the residue class of $\varphi \mod \theta O$. If $\varphi \equiv \varphi_2 \mod \theta O$, then $\varphi(\beta_1 - \beta_2)/\theta = x_1 + x_2\alpha + \cdots + x_i\alpha^{k-1}$ with $x_i \in \mathbb{Z}$, $i = 1, \ldots, k$. So, $L_k(\beta_1 - \beta_2)/\theta = x_k$. Hence, 

$$\frac{\chi_{\varphi}(\beta_1)}{\chi_{\varphi}(\beta_2)} = \exp(x_k) = 1.$$ 

We claim that if $\beta_1 \not\equiv \beta_2 \mod \theta O$, then $\chi_{\varphi} \not\equiv \chi_{\varphi_2}$. Indeed, $(\beta_1 - \beta_2)/\theta = a_1 + a_2\alpha + \cdots + a_k\alpha^{k-1}$ and at least one of the $a_i \in \mathbb{Q}\setminus\mathbb{Z}$. Let $m$ be the largest index such that $a_m \in \mathbb{Q}\setminus\mathbb{Z}$. Then $a_i \in \mathbb{Z}$ for $m < j \leq k$. Consider 

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

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

$$b = L_k(\frac{\beta_1 - \beta_2}{\theta} \alpha^{k-m}) \in \mathbb{Q}\setminus\mathbb{Z}.$$ 

Thus, $\chi_{\varphi}(\alpha^{k-m}) \not\equiv \chi_{\varphi_2}(\alpha^{k-m})$. Therefore, we have found all characters, since there are as many as $\mathcal{A}(\theta O)$ 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 $\mathbb{Q}(\alpha)$ 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 $\varphi : O \rightarrow O/I$ be the natural homomorphism and $\psi : O/I \rightarrow \{0, \cdots, \mathcal{N}I-1\}$ such that $\psi(r + I) = r$ for $r = 0, \cdots, \mathcal{N}I-1$. The characters of $O/I$ are given by 

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

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 $\mathcal{N}\mathcal{P} = p^l$ and let $\varphi$ be the natural homomorphism from $O$ to $O/\mathcal{P}$. We write $\varphi(\alpha) = \alpha$. Then the characters of $O/\mathcal{P}$ are given by 

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

http://escholarship.lib.okayama-u.ac.jp/mjou/vol18/iss1/2
where $\alpha \in O/\mathcal{I}$.

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 $\mathcal{I} \neq \emptyset$, $\mathcal{F}$ be countable collections of closed subgroups of $G$ such that:

(i) finite intersections of elements of $\mathcal{I} \cup \mathcal{F}$ are of compact index;

(ii) for each $S \in \mathcal{I}$ and $T \in \mathcal{F}$, we have $S \subseteq T$;

(iii) for each $T \in \mathcal{F}$, there exists a character $\chi_T$ of $G$ such that $\chi_T$ is trivial on $T$ but is nontrivial on each $S \in \mathcal{I}$.

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

**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 $m, n=1, 2, \ldots$ and $J_n^*$ is principal for $n=1, 2, \ldots$. Then there exists a sequence in $O$ which is u.d. mod $I_m$ for $m=1, 2, \ldots$, but which, for $n=1, 2, \ldots$, is not u.d. mod $J_n$.

**Proof.** We put $\mathcal{I} = \{I_m\}$, $m=1, 2, \ldots$, and $\mathcal{J} = \{J_n\}$, $n=1, 2, \ldots$, 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 $J_n^* = rO$ for some $r \in J_n^*$. Then the character $\chi_r(\alpha) = \exp(\operatorname{Tr}_{K/O}(\alpha r))$, $\alpha \in O$, is trivial on $J_n$. Suppose $\chi_r(\alpha)$ were trivial on some $I_m$. It follows that $r \in I_m^*$. Thus, $J_n^* = rO \subseteq I_m^*$, which implies $I_m \subseteq J_n$, a contradiction.

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

**Proof.** Let $f$ be the minimal polynomial of $\alpha$ over $\mathbb{Q}$. Then $O^* = (f'(\alpha))^{-1}O$ (see [12, p.164]). Thus, $(\theta_n O)^* = (\theta_n f'(\alpha))^{-1}O$, which is principal for $n=1, 2, \ldots$. 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 $O^* = \prod_{i=1}^s \mathcal{P}_i^{-r_i}$ with $r_i > 0$ for $1 \leq i \leq s$.
Let $h$ be the class number of $K$, and let $\mathfrak{a}_1 \neq \mathfrak{a}_2$ be two prime ideals that are both distinct from $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$. Put

$$J = \mathfrak{a}_1^h \mathfrak{a}_2^h \prod_{i=1}^r \mathfrak{p}_i^{(v_i - 1)\nu_i}.$$ 

We note that $I_n \subseteq J$ for $m = 1, 2, \cdots$ since $J$ is not a power of a prime ideal, and that $J^* = J^{-1}O^* = (\mathfrak{a}_1^{-1} \mathfrak{a}_2^{-1} O^*)^h$, 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 $\tau^tO_p$ with $t \in \mathbb{Z}$. 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 $\lambda \in K_p$ has a unique expansion $\delta = \sum_{i=1}^{\infty} \alpha_i \tau^i$, $\nu_i \in \mathbb{Z}$, with $\alpha_i \neq 0$ for $\delta \neq 0$ and $\alpha_i \in \mathfrak{R}$ for $i \geq r$, where $\mathfrak{R}$ is a fixed complete system of representatives of $O/\mathfrak{P}$ (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 $\Delta$ is u.d. in $O_p$ if $\Delta$ is u.d. mod $\tau^tO_p$ (in the obvious sense) for all positive integers $t$.

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

**Proof.** For $\alpha, \beta \in O$, we have $\alpha \equiv \beta \pmod{\tau^tO_p}$ if and only if $\nu_p(\alpha - \beta) \geq t$ if and only if $\alpha \equiv \beta \pmod{\mathfrak{P}_t}$. Hence, $A(N, \beta + \mathfrak{P}_t, \mathcal{A}) = A(N, \beta + \tau^tO_p, \mathcal{A})$. So,

$$\lim_{\mathcal{A} \to \infty} \frac{A(N, \beta + \mathfrak{P}_t, \mathcal{A})}{N} = \lim_{\mathcal{A} \to \infty} \frac{A(N, \beta + \tau^tO_p, \mathcal{A})}{N}$$

whenever one of the two limits exists; thus, $\mathcal{A}$ is u.d. mod $\mathfrak{P}_t$ if and only if $\mathcal{A}$ is u.d. mod $\tau^tO_p$. 

http://escholarship.lib.okayama-u.ac.jp/mjou/vol18/iss1/2
The following two corollaries are immediate consequences.

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

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

Let $\delta=\sum_{i=r}^{m} \alpha_i \tau^i$ 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 $\Delta=(\delta_n)$, $n=1, 2, \ldots$, be a sequence of elements of $O_p$. Then $\Delta$ is u.d. in $O_p$ if and only if for each $m=0, 1, \ldots$, the sequence $(S_m(\delta_n))$, $n=1, 2, \ldots$, is u.d. mod $P^{m+1}$ in $O$.

**Proof.** Let $\delta_n=\sum_{i=0}^{m} \alpha_n \tau^i$ for $n=1, 2, \ldots$. Since $\delta_n-S_m(\delta_n)=\sum_{i=m+1}^{\infty} \alpha_n \tau^i \in \tau^{m+1}O_p$, the sequence $\Delta$ is u.d. mod $\tau^{m+1}O_p$ if and only if $(S_m(\delta_n))$, $n=1, 2, \ldots$, is u.d. mod $P^{m+1}$ in $O$. Consequently, $\Delta$ is u.d. in $O_p$ if and only if $(S_m(\delta_n))$, $n=1, 2, \ldots$, is u.d. mod $P^{m+1}$ in $O$ for $m=0, 1, \ldots$.

Let $\mathcal{C}$ denote the Cartesian product $O = \times_{P} O_{P}$, where $P$ runs through the set of all nontrivial discrete prime divisors of $K$. Let $\mathcal{C}$ be furnished with the product topology. Then $\mathcal{C}$ is a second countable compact group with respect to coordinatewise addition. $\mathcal{C}$ can also be viewed as a subgroup of the adèle ring of $K$. Let $\mu$ be the Haar measure on $\mathcal{C}$. Then a $\mu$-u.d. sequence in $\mathcal{C}$ is simply said to be u.d. in $\mathcal{C}$ (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 $P, \mathcal{P}, \ldots$. For $j \geq 1$, let $\tau_j\in O$ such that $\nu_{P_j}(\tau_j)=1$. By a fundamental neighborhood in $\mathcal{C}$, we mean a set $V \subseteq \mathcal{C}$ of the form $V=\times_{j=1}^{j=1} V_{j}$, 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 $\Gamma=(\gamma_n)$, $n=1, 2, \ldots$, is u.d. in $\mathcal{C}$ if and only if

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

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

Produced by The Berkeley Electronic Press, 1975
H. NIEDERREITER and S.K. LO

Proof. Evidently, a fundamental neighborhood $V$ in $\mathcal{O}$ is simultaneously closed and open. Thus, $V$ is a $\mu$-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 $\mu$, for any $\epsilon > 0$ there exists a closed set $C \subseteq E$ with $\mu(E \setminus C) < \epsilon$. Let $\{V_i\}, V_i \subseteq E$, be an open cover for $C$ consisting of fundamental neighborhoods. By the compactness of $C$, there exists a finite subcover $\{V_1, \ldots, V_r\}$. Then $\mu(E \setminus \bigcup_{j=1}^{r} V_j) < \epsilon$. 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 $\mu$. So, the sufficiency is proved.

Let $i_p : O \to \mathcal{O}$ be the canonical embedding. Then $i = \prod_{p \in O} i_p : O \to \mathcal{O}$ 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 $\alpha$ to denote $\alpha, i_p(\alpha)$, 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 $I = \prod_{j=1}^{r} \mathcal{P}_{j}^{s_j}$ with $s_j \geq 0$ for $j = 1, \ldots, r$.

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

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

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

Proof. Suppose $\mathcal{A}$ 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, $A(N, \beta + I, \mathcal{A}) = A(N, V, \mathcal{A})$, and so

$$
\lim_{\beta \to \infty} \frac{A(N, \beta + I, \mathcal{A})}{N} = \lim_{\beta \to \infty} \frac{A(N, V, \mathcal{A})}{N} = \mu(V) = \frac{1}{N}. 
$$
by Lemma 3.6. Thus, $\mathcal{A}$ is u.d. in $O$.

Conversely, suppose $\mathcal{A}$ is u.d. in $O$. Let $V$ be a fundamental neighborhood in $\mathcal{O}$, say $V = \bigtimes_{j=1}^{r} V_j$, with $V_j = \beta_j + \tau_j O_{\beta_j}$ for $j = 1, \ldots, r$ and $V_j = O_{\beta_j}$ for $j > r$, where $\beta_j \in O$ for $j = 1, \ldots, r$. By the Chinese Remainder Theorem, there exists a $\beta \in O$ with $\beta_j \equiv \beta_j \pmod{\mathbb{Z}_{\beta_j^r}}$ for $j = 1, \ldots, r$. Then, with $I = \prod_{j=1}^{r} \mathbb{Z}_{\beta_j^r}$, we have $A(N, V, \mathcal{A}) = A(N, \beta + I, \mathcal{A})$ according to Lemma 3.7. It follows that

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

and so $\mathcal{A}$ is u.d. in $\mathcal{O}$ by Lemma 3.6.

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

Let $\mathcal{B}$ be the algebra generated by the empty set and the cosets of nonzero ideals of $O$. A finitely additive measure $\nu$ called the Banach-Buck measure (see [9, Section 4]) can be defined on $\mathcal{B}$. Let $\nu^*$ be the outer measure which extends $\nu$. 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 $\mathcal{O}$. 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 $\mathcal{O}$. 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 $O = \mathbb{Z}$, 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 \([K : \mathbb{Q}] \geq 2\). The case \(K = \mathbb{Q}\) was proved by Niven [10]. We shall construct a normed regular Borel measure \(\mu_1\) on \(\mathcal{O}\) which is different from the Haar measure \(\mu\) but has the same projections as \(\mu\) has on each coordinate space \(O_p\). Since \(O\) is dense in \(\mathcal{O}\), it can be arranged into a \(\mu\)-u.d. sequence \(\mathcal{A}\). However, \(\mu_1\) is different from \(\mu\), and so \(\mathcal{A}\) is not u.d. in \(O\). Since \(\mu\) and \(\mu_1\) have the same projection on each \(O_p\), \(\mathcal{A}\) is u.d. in each \(O_p\). By Corollary 3.3, this means that \(\mathcal{A}\) is u.d. modulo all powers of all prime ideals in \(O\).

For the sake of brevity, we only sketch the construction of \(\mu_1\). By choosing two prime ideals in \(O\) that lie over a rational prime splitting completely in \(K\), we obtain prime ideals \(\mathcal{P}_1\) and \(\mathcal{P}_2\) with \(\mathcal{N}\mathcal{P}_1 = \mathcal{N}\mathcal{P}_2 = q\), say. By a square of degree \(r\) in \(O_{\mathcal{P}_1} \times O_{\mathcal{P}_2}\), we mean a Cartesian product of cosets of the form \((\alpha + \tau_1^{r} O_{\mathcal{P}_1}) \times (\beta + \tau_2^{r} O_{\mathcal{P}_2})\), \(\alpha \in O_{\mathcal{P}_1}\), \(\beta \in O_{\mathcal{P}_2}\), \(r\) a positive rational integer. We label the distinct cosets of \(\tau_1^{0} O_{\mathcal{P}_1}\) by \(r_1^{0}, \ldots, r_{q-1}^{0}\), \(\tau_2^{0} O_{\mathcal{P}_2}\) by \(r_1^{0}, \ldots, r_{q-1}^{0}\), \(\tau_1^{1} O_{\mathcal{P}_1}\) by \(r_1^{1}, \ldots, r_{q-1}^{1}\), and \(\tau_2^{1} O_{\mathcal{P}_2}\) by \(r_1^{1}, \ldots, r_{q-1}^{1}\). Then \((\alpha + \tau_1^{0} O_{\mathcal{P}_1}) \times (\beta + \tau_2^{0} O_{\mathcal{P}_2})\) 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 \(\mathcal{G}\) be the algebra generated by all the squares in \(O_{\mathcal{P}_1} \times O_{\mathcal{P}_2}\). Define a set function \(\varphi_1\) from the generators of \(\mathcal{G}\) to the nonnegative reals by

\[
\varphi_1((\alpha + \tau_1^{r} O_{\mathcal{P}_1}) \times (\beta + \tau_2^{r} O_{\mathcal{P}_2})) = q^{-n}
\]

if \((\alpha + \tau_1^{r} O_{\mathcal{P}_1}) \times (\beta + \tau_2^{r} O_{\mathcal{P}_2})\) is a diagonal square of degree \(n\) and

\[
\varphi_1((\alpha + \tau_1^{r} O_{\mathcal{P}_1}) \times (\beta + \tau_2^{r} O_{\mathcal{P}_2})) = 0 \text{ otherwise.}
\]

It can be proved that \(\varphi_1\) can be extended uniquely to a normed regular Borel measure \(\varphi_1\) on \(O_{\mathcal{P}_1} \times O_{\mathcal{P}_2}\). Evidently, \(\varphi_1\) is distinct from the Haar measure on \(O_{\mathcal{P}_i} \times O_{\mathcal{P}_j}\), but has the same projections on \(O_{\mathcal{P}_i}\) for \(i = 1, 2\) as the Haar measure. We let \(\varphi_2\) be the Haar measure on \(\bigotimes_{i=1}^{2} O_{\mathcal{P}_i}\) and set \(\mu_1 = \varphi_1 \times \varphi_2\). Then \(\mu_1\) is the desired measure.

4. Uniform distribution of algebraic integers and of rational integers. Since the uniform distribution in \(\mathbb{Z}^k\) 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 \(\mathbb{Z}^k\).
Theorem 4.1. (Niederreiter). Let $K$ be an algebraic number field with integral basis $\{\omega_1, \cdots, \omega_n\}$ over $\mathbb{Q}$ and let $\mathcal{O} = (\alpha_n)$, $n=1, 2, \cdots$, with $\alpha_n = \sum_{i=1}^n x_{n,i} \omega_i$ for $n \geq 1$, be a sequence in $O$. The sequence $\mathcal{O}$ 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 $(\sigma_n)$, $n=1, 2, \cdots$, with $\sigma_n = s_1 x_{n,1} + \cdots + s_k x_{n,k}$ for $n \geq 1$, are u.d. in $\mathbb{Z}$.

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 $\mathcal{O} I$ of a certain sequence in $\mathbb{Z}$ 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 $\{\omega_1, \cdots, \omega_n\}$ over $\mathbb{Q}$, 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. $m = \mathcal{O} I$;
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 $d_i \in \mathbb{Z}$, 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 $m \equiv I$, we have $m \alpha \equiv 0 \pmod{I}$, and so $\mathcal{O} I$ divides $m$. On the other hand, $m \leq \mathcal{O} I$, 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 $d \in \mathbb{Z}$, and (1) follows.

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

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

Produced by The Berkeley Electronic Press, 1975
Proof. If $a$ is a real number, we use $\langle a \rangle$ to denote the smallest rational integer $\geq a$. Suppose $\mathcal{P}$ lies over the rational prime $p$. Let $n$ be a positive integer such that $n \in \mathcal{P}^i$. This is equivalent to $\nu_p(n) \geq t/e$. Thus the smallest positive rational integer $m$ in $\mathcal{P}^i$ is $m = p^{t/e}$. By Theorem 4.2, $O/\mathcal{P}^i$ is cyclic if and only if $tf = \langle t/e \rangle$ (since $m \mathcal{P}^i = p^t$). 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 $\langle t/e \rangle < t/e + 1 < t/tf$.

Theorem 4.4. Suppose $I = \prod_{i=1}^r \mathcal{P}_i$, where the $\mathcal{P}_i$ 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 $\text{g.c.d.}(\mathcal{P}_i, \mathcal{P}_j) = 1$ 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 $O/I = \bigoplus_{i=1}^r (O/\mathcal{P}_i)$. Thus, the sufficiency is a direct consequence of Theorem 4.3 and of $\text{g.c.d.}(\mathcal{P}_i, \mathcal{P}_j) = 1$ for $i \neq j$.

As for the necessity, one notices first that $O/\mathcal{P}_i$ is cyclic for $i = 1, \ldots, r$. 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 $\mathcal{P}_1 = p^t$ and $\mathcal{P}_2 = p^r$. Since $O/I = (O/\mathcal{P}_1 \mathcal{P}_2) \oplus (O/\prod_{i=3}^r \mathcal{P}_i)$, it suffices to show that $O/\mathcal{P}_1 \mathcal{P}_2$ 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 $\mathcal{P}_1 \mathcal{P}_2$ 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 $\mathcal{P}_1 \mathcal{P}_2$ is $m = \max_{i=1,2} \langle t_i/e_i \rangle$. By Theorem 4.2, $O/\mathcal{P}_1 \mathcal{P}_2$ is cyclic if and only if $\max_{i=1,2} \langle t_i/e_i \rangle = f_1 t_1 + f_2 t_2$. However, it is obvious that $\max_{i=1,2} \langle t_i/e_i \rangle < f_1 t_1 + f_2 t_2$, and this yields the desired contradiction.

Theorem 4.5. Let $K$ be an algebraic number field with integral basis $\{\omega_1, \ldots, \omega_k\}$ over $\mathbb{Q}$, and let $I$ be a nontrivial integral ideal. Suppose $\omega_i \equiv d_i \pmod{I}$ for $1 \leq i \leq k$, where $d_i \in \mathbb{Z}$ for $1 \leq i \leq k$. Then a sequence $\alpha = (\alpha_n) = (a_0, a_1, \ldots)$ in $O$ with $\alpha_n = x_1 \omega_1 + \cdots + x_k \omega_k$ for $n \geq 1$ is u.d. mod $I$ if and only if the sequence $\sigma = (\sigma_n) = (a_0, a_1, \ldots)$ in $\mathbb{Z}$, with $\sigma_n = x_1 d_1 + \cdots + x_k d_k$ for $n \geq 1$, is u.d. mod $I$ in $\mathbb{Z}$.
Proof. Since $\sigma_n \equiv \alpha_n \pmod{I}$, the sequence $\mathcal{A}$ can be replaced mod $I$ by the sequence $(\sigma_n)$, $n=1,2,\ldots$. According to Theorem 4.2, $\{0,1,\ldots,\mathcal{N}^I-1\}$ constitutes a complete system of representatives of $\mathcal{O}/I$, and if $d \in \mathcal{Z}$, we have

$$A(N, d \div I, (\sigma_n)) = A(N, d \div (\ldots \div I)^n, (\sigma_n)),$$

since $a \equiv b \pmod{I}$ is equivalent to $a \equiv b \pmod{\ldots \div I}$ for $a, b \in \mathcal{Z}$. Thus, the theorem follows.

**Corollary 4.6.** Suppose $K = \mathbb{Q}(\alpha)$ with integral basis $\{1, \alpha, \ldots, \alpha^{k-1}\}$ over $\mathbb{Q}$ and $I$ is a nontrivial integral ideal with $\alpha \equiv d \pmod{I}$ for some $d \in \mathcal{Z}$. Then a sequence $\mathcal{A} = (\alpha_n), n=1,2,\ldots$, in $\mathcal{O}$ with $\alpha_n = x_n + \sum_{i=1}^{k-1} x_{n,i}\alpha^i$ for $n \geq 1$ is u. d. mod $I$ if and only if the sequence $(\sigma_n)$, $n=1,2,\ldots$, where $\sigma_n = x_{n,0} + x_{n,1}d + \sum_{i=1}^{k-1} x_{n,i}d^{i-1}$ for $n \geq 1$, is u. d. mod $\ldots \div I$ in $\mathcal{Z}$.

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

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

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

$$\sigma_n = \frac{1}{m} \left(j_1m_{x_{n,1}} \cdots m_{x_{n,k}} \cdots + j_1m_{1} \cdots m_{k-1}x_{n,k}\right) \text{ for } n \geq 1,$$

are u. d. mod $\left(\frac{1}{m} \Pi_i m_i \right)$ in $\mathcal{Z}$ for any $k$-tuple $(j_1, \ldots, j_k) \neq (0, \ldots, 0)$ in $\mathcal{Z}^k$ with $0 \leq j_i \leq m_i$ for $1 \leq i \leq k$ and $m = \text{g. c. d.} \left(\Pi_i m_i, j_1m_{1} \cdots m_{k-1}\right)$.

**Proof.** To prove necessity, let $t \in \mathcal{Z}$ with $1 \leq t < \frac{1}{m} \Pi_i m_i$ and set
\[
\frac{t}{\prod_{i=1}^{k} m_i} = \frac{p}{q}, \quad \text{where g. c. d.} \ (p, q) = 1 \quad \text{and} \quad q \geq 1.
\]

Obviously, \( q > 1 \). Put
\[
s_1 = \frac{j_1 m_1 \cdots m_k}{m}, \ldots, \ s_k = \frac{j_k m_1 \cdots m_k}{m}.
\]

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 \( q \big| \frac{1}{\prod_{i=1}^{k} m_i} \), which implies that \( qm \) is a common divisor of \( \prod_{i=1}^{k} m_i, j_1 m_1 \cdots m_k, \ldots, j_k m_1 \cdots m_k \). But \( qm > m \), yielding a contradiction. Thus, by [7, Theorem 2.1], one has
\[
\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \exp \left( \frac{1}{\prod_{i=1}^{k} m_i} \left( s_1 x_{n1} + \cdots + s_k x_{nk} \right) \right) = 0,
\]
and the desired conclusion follows from [3, Chapter 5, Theorem 1.2].

To prove sufficiency, let \( (j_1, \ldots, j_k) \) be as in the theorem. Then,
\[
\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \exp \left( \frac{j_1}{m_1} x_{n1} + \cdots + \frac{j_k}{m_k} x_{nk} \right) = 0,
\]
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 \( \{ \omega_1, \ldots, \omega_k \} \) over \( \mathbb{Q} \). If \( I = m_1 \omega_1 \mathbb{Z} \oplus \cdots \oplus m_k \omega_k \mathbb{Z}, \ m_i \in \mathbb{Z}, \ m_i \geq 1 \) for \( i = 1, \ldots, k, \) is a nontrivial integral ideal and \( \mathfrak{N} = (\alpha_n), \ n = 1, 2, \ldots, \) with \( \alpha_n = x_{n1} \omega_1 + \cdots + x_{nk} \omega_k \) for \( n \geq 1, \) is a sequence of algebraic integers, then \( \mathfrak{N} \) is u. d. mod \( I \) if and only if the sequences \( (\sigma_n), \ n = 1, 2, \cdots, \) with
\[
\sigma_n = \frac{1}{m} (j_1 m_1 \cdots m_k x_{n1} + \cdots + j_k m_1 \cdots m_k x_{nk}) \quad \text{for} \quad n \geq 1,
\]
are u. d. mod \( \left( \frac{\cdot}{m} \right) \) in \( \mathbb{Z} \) for every \( k \)-tuple \( (j_1, \ldots, j_k) \neq (0, \ldots, 0) \) in \( \mathbb{Z}^k \) with \( 0 \leq j_i < m_i \) for \( 1 \leq i \leq k \) and \( m = \text{g. c. d.} \left( \left\lceil \frac{1}{\cdot} \right\rceil, j_1, m_1 \cdots m_k, \ldots, j_k m_1, \ldots m_k \right) \).

**REFERENCES**


**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)*