On normal sets of numbers

by

ALAN ZAME (Coral Gables, Fla)

0. Introduction. In [4], M. Mendès-France introduced the notion of a normal set of numbers and showed that the complement of a finite extension of the rationals is normal. His proof makes use of some fundamental properties of the Pisot–Vijayaraghavan numbers. In [5], Y. Meyer obtained some results which have applications to normal sets by making essential use of some non-elementary harmonic analysis, harmonic sets and Fourier transforms in particular. The purpose of this paper is to give an elementary proof of an extension of Meyer’s result on normal sets and to obtain some results on countable normal sets.

1. Preliminaries. We assume that the reader is familiar with the usual definitions and basic properties of the theory of uniform distribution mod 1 (u.d. mod 1). (See [1] for references.) A set \( M \) of real numbers is said to be normal if there exists a sequence \( A = \{\lambda_n\} \) of real numbers such that \( Ax = \{\lambda_n x\} \) is u.d. mod 1 if and only if \( x \in M \). A normal set \( M \) must obviously satisfy

(i) \( 0 \in M \),

(ii) \( x \in M, n \in \mathbb{Z} \setminus \{0\} \rightarrow nx \in M \)

(where \( \mathbb{Z} \) = integers and, if \( A \) and \( B \) are sets then \( A \setminus B \) denotes their difference).

Additionally, if we require the sequence \( A \) to consist of integers (in which case we will call \( M \) integer-normal) we must also have

(iii) \( Q \cap M = \emptyset \) (\( Q \) rationals),

(iv) \( M + Z = M \) (where \( A + B = \{a + b\} \) and either \( \mu(M) = 0 \) or \( \mu(R \setminus M) = 0 \) (where \( R \) = reals and \( \mu \) = Lebesgue measure).

(This last property is a consequence of the “zero-one” law or of ergodic theory.) However, simple counting arguments show that the conditions listed above are not sufficient. There are cases, though, in which conditions (i) and (ii) are sufficient for normality, as we shall see.

If \( A \) is a sequence and \( I \) is an interval we shall say that \( A \) is u.d. in \( I \) if all the terms of \( A \) belong to \( I \) and if for every subinterval \( J \subseteq I \)

\[
\lim_{N \to \infty} \frac{1}{N} \text{ (number of } \lambda_k \text{ in } J, 1 \leq k \leq N) = [J]||I||,
\]

where \([I]\) = length of \( I \). If \( A \) is not u.d. mod 1 but does have a distribution function we shall write “\( A \) is d. mod 1.” Finally, if \( A \) is d. mod 1 and the limits in question exist uniformly (as in the definition of a well-distributed sequence) we shall write “\( A \) is d.w. mod 1.”

We shall need the following lemmas:

**Lemma 1.** (i) If \( U \) is d.w. mod 1, \( kU \in \mathbb{Z} \setminus \{0\} \), then \( kU = (ku_n) \) is u.d. mod 1. If \( U \) is well distributed mod 1 (w.d. mod 1) then so is \( kU \).

(ii) If \( a, b \) are real numbers such that \( 0 < a < b \leq 1 \) and \((n_b)\) is the increasing sequence of all positive integers \( n \) for which \( na \in [a, b] \) mod 1, then \((n_b)\) is w.d. mod 1.

(iii) Under the conditions of (ii), if \( 0 < a < b \leq 1 \) and \((n_b)\) is the increasing sequence of all positive integers \( n \) for which \( na \in [a, b] \) mod 1, then \((n_b)\) is w.d. mod 1.

(iv) If \( U \) is u.d. in \([0, a]\) and \( v \) is a real number then the sequence \( rv \) has a distribution function mod 1, and \( vU \) is u.d. mod 1 \( \iff rv \in \mathbb{Z} \setminus \{0\} \). If \( U \) is u.d. in \([0, a]\) and \( vU \) is d.w. mod 1 unless \( rv \in \mathbb{Z} \setminus \{0\} \). Similarly, if \( U \) is w.d. in \([0, a]\) and \( rv \) is an integer, then \( U \) is w.d. mod 1 if and only if \( ra \in \mathbb{Z} \setminus \{0\} \).

Proof. (i) and (ii) are well known. (iii) is an easy consequence of (ii) and the proof of (iv) is straightforward.

In passing we note that (iv) shows that \( \mathbb{Z} \setminus \{0\} \) is a normal set: If \( A \) is u.d. in \([0, 1]\), then \( A / \mathbb{Z} \) is u.d. mod 1 \( \iff xA \subset \mathbb{Z} \setminus \{0\} \).

**Lemma 2.** Let \( A_1, A_2, \ldots \) be disjoint, increasing sequences of real numbers and let \( A = (\lambda_k) \) be an increasing sequence such that each \( \lambda_k \) belongs to some \( A_i \).

\[
\lim_{N \to \infty} \frac{1}{N} \text{ (number of } \lambda_k \text{ in } A_i, 1 \leq k \leq N) = \nu_i \quad (i = 1, 2, \ldots)
\]

where \( \nu_i > 0 \), \( \sum \nu_i = 1 \), and such that the terms of \( A \) belonging to \( A_i \) consist of segments of \( A_i \) of lengths tending to \( \infty \). (Note that if \( \lim A_i = \infty \) for each \( i \) then it is possible to construct such a \( A \).) Then

(i) If each \( A_i \) is w.d. mod 1 then \( A \) is w.d. mod 1.

(ii) If some \( A_i \) is d.w. mod 1 and the other \( A_i \) are w.d. mod 1 then \( A \) is not u.d. mod 1.

Proof. The proof will be left to the reader.

2. **Theorem 1.** Let \( M \) be a countable set of reals such that \( QM + Q = M \).

(i) There exists a strictly increasing sequence of integers \( \lambda \) such that \( xA \) is n.d. mod 1 \( \iff x \in M \).

(ii) For each \( \varepsilon > 0 \) there exists a sequence \( \lambda \), where \( |\lambda_k - k| < \varepsilon \), such that \( xA \) is u.d. mod 1 \( \iff x \in M \).

In particular, if \( M = K \setminus V \), where \( V \) is a countable dimensional vector space over \( Q \) which contains \( Q \), then \( M \) is integer-normal. (Cf. [5], Theorems 8 and 9.)

Proof. Let \( M \) be the set described in the theorem. We may find a countable set \( S = (\alpha) \subseteq M \setminus Q \) which has the property that for \( i \neq j \) the three numbers 1, \( s_i, s_j \) are linearly independent over \( Q \) and such that \( M = QS + Q \). Let \( a \) be some fixed irrational number, 0 < \( a < 1 \). We may assume that \( S \neq \emptyset \), for the case \( M = Q \) is well known (let \( A = (\alpha) \)). For each \( i \) let \( \bar{A}_i \) be the sequence of positive integers \( n_i \) in increasing order, for which \( na \in [0, a] \) mod 1. Choose subsequences \( A_i \) of \( \bar{A}_i \) such that the sequences \( A_i \) and \( A_j \) have no elements in common for \( i \neq j \) and such that \( A_i \) is composed of segments of \( A_i \) of lengths tending to \( \infty \). Finally, choose \( A \) to satisfy the hypotheses of Lemma 2. We claim that \( xA \) is u.d. mod 1 \( \iff x \in M \).

First, suppose \( xA \notin M \). If \( x \) is rational then \( xA \) is certainly not u.d. mod 1 since \( A \) is a sequence of integers. Suppose, then, that \( x \) is irrational and \( A \) is u.d. mod 1. Then \( x = p + \alpha_1/q \) for some integer \( p \) and rational \( \alpha_1 \). Because of Lemma 1 (i), \( (ka)A \) is u.d. mod 1 for every \( k \in \mathbb{Z} \setminus \{0\} \), whereas there exists \( y_1 = \lambda_1, y_2 \in \mathbb{Z} \setminus \{0\} \) such that \( y_1A \) is u.d. mod 1. By Lemma 1 (iii) the sequence \( y_1A \) is w.d. mod 1 for \( j \neq i \), so that \( y_1A \) is w.d. mod 1 if \( j \neq i \). However, \( s_iA_i \leq [0, a_i] \) mod 1 and, in fact, the sequence \( \{s_i, s_j\} \) is w.d. in \([0, a_i]\) \( (|\beta| = \text{ fractional part of } \beta) \). It follows that the same is true for \( s_iA_i \) and thus, by Lemma 1 (iv) the sequence \( y_1A \) is d.w. It follows from Lemma 2 (ii) that \( y_1A \) is not u.d. mod 1, a contradiction.

Now, suppose \( xA \in M \). Then, for each \( i \), the three numbers 1, \( x, s_i \) are linearly independent over \( Q \) whence, by Lemma 1 (iii) again, we see that \( xA \), is a.e. mod 1. Lemma 2 (i) shows that \( xA \) is u.d. mod 1.

This proves the first part of the theorem. The proof of the second part is similar once we have constructed the sequences \( \bar{A}_i \) as follows: Let \( k \) be a fixed integer \( > 1/\varepsilon \) and let \( \alpha_i = 1 - s_i/k \). For each \( i \) let \( \bar{A}_i = (\lambda_n) \) be the sequence chosen as follows:

\[
\lambda_n = \begin{cases} n & \text{ if } n s_i \epsilon [0, a_i] \mod 1, \\ n + 1/k & \text{ if } n s_i \epsilon [a_i, 1] \mod 1. \end{cases}
\]
The details will be omitted.

We remark at this point that if we are only interested in normality the conditions on $\mathcal{M}$ can be weakened.

**Proposition 2.** Let $M \leq \mathbb{R}$ be a countable non-empty set, with $QM = M$. Then $R \setminus M$ is a normal set.

**Proof.** We may assume that $M \neq \{0\}$ (the sequence $\sqrt{n}x$ is u.d. mod 1 for all $x \neq 0$). Let $S \subseteq M$ be such that $M = QS$ and any two distinct elements of $S$ are linearly independent over $Q$. For each $i$, let $A_i$ be the sequence $\{i(1/k)\}$. Then $xA_i$ is u.d. mod 1 is not a rational multiple of $s_i$. If $x$ is a rational multiple of $s_i$ then $xA_i$ is d.w. We can now finish the proof by forming $A$ as in the proof of Theorem 1.

3. Proposition 2 shows that certain large sets are normal. In this section we shall use different methods to show that certain small sets are normal.

**Lemma 3.** Let $M \leq \mathbb{Z}$ be such that

(i) $0 \not\in M$,

(ii) $nM \subseteq M$ if $n \in \mathbb{Z} \setminus \{0\}$.

Then there exists a sequence $U = (u_n)$ such that $rU$ is u.d. mod 1 for every integer $r$.

Furthermore, if $rM$ then

$$\lim_{p \to \infty} \frac{1}{p} \sum_{k=1}^{p} e^{2\pi i u_n k} > 0.$$

**Proof.** Let $\mu$ be the Lebesgue measure on $[0, 1]$. Define the continuous function $f$ on $[0, 1]$ by

$$f(x) = 1 + \sum_{n \in M} \frac{1}{2^n \cos 2\pi n x}.$$

We may also write

$$f(x) = 1 + \sum_{n \in M} \frac{1}{2^n \cos 2\pi n x}.$$

because of the symmetry of $M$. Thus we see that $f > 0$ on $[0, 1]$. Let $\nu$ be the regular Borel probability measure on $[0, 1]$ defined by $d\nu = f d\mu$.

We observe that the $n$th Fourier coefficient of $\nu \ast (n)$, is $0 \iff n \in M$.

Since $[0, 1]$ is a compact metric space and $\nu$ is a probability measure on $[0, 1]$, there exists a sequence $V$ in $[0, 1]$ such that $V$ is i.u.d., i.e., for every continuous function $g$ on $[0, 1]$ we have

$$\lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} g(v_k) = \int g(x) d\nu(x).$$

If $n$ is an integer we claim that $nV$ is u.d. mod 1 $\iff n \in M$. For $nV$ is u.d. mod 1 $\iff$ for every positive integer $p$

$$L(p) = \lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} e^{2\pi i p n k} = 0.$$

But, by (*), $L(p) = p \nu \ast (-p)$ and this vanishes for all positive $p \not\in M$.

Now, let $W = (w_n)$ be a sequence which is u.d. in $[0, 1]$. Let $(n_k)$ be a sequence of integers such that

$$n_k/(n_1 + \ldots + n_{k-1}) \to \infty,$$

and let $U$ be the sequence $(u_n)$, where

$$u_n = \begin{cases} v_n & \text{if } n_n \leq n = n_r + j - 1 < n_{r+1}, r \text{ odd,} \\ w_n & \text{if } n_n \leq n = n_r + j - 1 < n_{r+1}, r \text{ even.} \end{cases}$$

Then the sequence $U$ will have the desired properties. In fact, the analogue of Lemma 1 (iv) for exponential sums shows that the

$$\lim_{N_r \to \infty} \frac{1}{N_r} \sum_{k=1}^{N_r} e^{2\pi i u_n k} > 0 \text{ for } r \in \mathbb{Z} \setminus M$$

when $N_r$ runs through the sequence $(n_k)$ and for $r \in \mathbb{Z} \setminus M$ when $N_r$ runs through the sequence $(n_{k+1})$.

**Definition.** Let $U_1, \ldots, U_k$ be sequences, say $U_i = (w_{i,j})$. The sequence $U = U_1 \oplus \ldots \oplus U_k$ is defined as follows: Let $f$ be a bijection from the positive integers to all $k$-tuples of positive integers such that the set $\{f(1), \ldots, f(n^k)\}$ consists of all $k$-tuples of integers from 1 to $n$.

Let $u_n$ be defined by

$$u_n = w_{n_1}^{(1)} + \ldots + w_{n_k}^{(k)}$$

where $f(n) = (n_1, \ldots, n_k)$. Then $U = (u_n)$. (Of course, there are many choices for $f$ but our results will not depend on which one we actually choose.)

**Lemma 4.** Let $U_1, \ldots, U_k$ be sequences, at least one of which is u.d. mod 1. Then $U = U_1 \oplus \ldots \oplus U_k$ is u.d. mod 1. On the other hand, if there exists a strictly increasing sequence of integers $(N_r)$ such that

$$\lim_{r \to \infty} \frac{1}{N_r} \sum_{k=1}^{N_r} e^{2\pi i u_n k} = 0 \quad (j = 1, \ldots, k)$$

then $U$ is not u.d. mod 1.

**Proof.** Let $U = (u_n)$. Since $(n+1)^2/n^2 \to 1$ it is sufficient to evaluate the means

$$L(n) = \lim_{N \to \infty} \frac{1}{N^k} \sum_{k=1}^{N^k} e^{2\pi i u_n k}.$$
But
\[
\frac{1}{N^n} \sum_{p=1}^{N^n} e^{2\pi i n_p \alpha} = \left( \frac{1}{N} \sum_{p=1}^{N} e^{2\pi i p \beta_p} \right)^N \left( \frac{1}{N} \sum_{p=1}^{N} e^{2\pi i p \beta} \right)
\]

so the result follows.

**Theorem 3.** Let \( S_1, \ldots, S_k \) be subsets of \( \mathbb{Z} \setminus \{0\} \) such that \( nS_i \subseteq S_i \) if \( n \in \mathbb{Z} \setminus \{0\} \). Let \( a_1, \ldots, a_k \) be non-zero reals. Then \( \bigcup_{i=1}^{k} a_i S_i \) is a normal set.

**Proof.** For each \( i \) select sequences \( V_i = (v_i^n) \) and \( W_i = (w_i^n) \) as in the proof of Lemma 3 and let \( (n_r) \) be a rapidly increasing sequence, again as in the proof of Lemma 3. Let \( q_1, \ldots, q_k \) be \( 2^{\frac{k}{2}} \) \( q \)-tuples of \( 0 \)'s and \( 1 \)'s and let \( t_i^0 = \) the \( i \)th coordinate of \( q_i \). Define the sequences \( U_i (i = 1, \ldots, k) \) as follows:

\[
U_i = (u_i^n),
\]

where \( u_r = n = n_r + p < n_{r+1} \), \( r = s (\text{mod } 2^k) \), \( 0 \leq s \leq 2^k - 1 \), then

\[
u_i^n = \begin{cases} \frac{1}{a_i} v_i^n & \text{if } t_i^0 = 0, \\ \frac{1}{a_i} v_i^n & \text{if } t_i^0 = 1. \end{cases}
\]

We observe that \( aU_r \) is u.d. \( \text{mod } 1 \) if \( a \in S_i \). Let \( U = U_1 \oplus \cdots \oplus U_k \). The observations made above and the first part of Lemma 4 show that \( aU \) is u.d. \( \text{mod } 1 \) if \( a \in \bigcup_i S_i \). Suppose \( a \notin \bigcup_i S_i \). Let \( i \) be the integer, \( 1 \leq i \leq 2^k \), so that for every \( i \) for which \( 1 \leq i \leq k \),

\[
t_i^0 = \begin{cases} 0 & \text{if } x = n, \text{ some } n \in \mathbb{Z}, \\ 1 & \text{if } x \notin n. \end{cases}
\]

From the choice of \( i \) it follows that for each \( i \)

\[
\lim_{r \to \infty} \frac{1}{N} \sum_{p=1}^{N} e^{2\pi i p \beta} > 0.
\]

Therefore, by Lemma 4, \( aU \) is not u.d. \( \text{mod } 1 \).

**4. In this section we will prove**

**Theorem 4.** \( Q \setminus \{0\} \) is a normal set. (Thus, if \( a \) is a non-zero real, then \( aQ \setminus \{0\} \) is a normal set.)

The proof depends upon the following result:

**Lemma 5.** There exists a positive number \( d \) such that if \( x \) is any irrational number then the inequality

\[
|a - k/p| < 1/|p^{1+d}|
\]

has infinitely many solutions for \( k \) an integer, \( p \) a prime.

**Proof.** This follows from the theorem on page 177 of [7] upon taking \( r = q = N_1^{1/3}, \beta = N^{-1/3 + \epsilon} \). (This in fact shows that we may take \( d = 1/3 - \epsilon \), for any positive \( \epsilon \).) The result also follows easily from other results of Vinogradov (see [6] or [2]).

**Proof of Theorem 4.** Let \( d \) be as in Lemma 5. For each prime \( p \) let \( b_p = \lfloor p^{1/2} \rfloor \) and let \( B_p \) be the finite sequence \( p, 2p, \ldots, k_p p \). Let \( (n_p) \) be a sequence of integers so that

\[
n_p/(n_1 + \cdots + n_p) \to 1
\]

and let \( S \) be the sequence

\[\begin{align*}
B_2, B_3, \ldots, B_p, B_p, \ldots, B_p, \\
\end{align*}\]

where \( B_p \) occurs \( n_p \) times. Let \( U \) be any sequence u.d. in \([0, 1]\). Let \( V = S \oplus U \). We claim that \( aV \) is u.d. \( \text{mod } 1 \) if \( a \in Q \setminus \{0\} \).

Suppose that \( x \) is irrational. We see that if \( |x - k/p| < 1/|p^{1+d}| \) then \( (nx) < 1/p^{1/2} \) if \( n \in B_p \). From this it follows that

\[
\limsup_N \left| \sum_{r=1}^{N} e^{2\pi i n_r a} \right| = 1.
\]

Furthermore, since \( U \) is u.d. in \([0, 1]\),

\[
\lim_{N \to \infty} \frac{1}{N} \left| \sum_{r=1}^{N} e^{2\pi i n_r a} \right| = \int_{0}^{1} e^{2\pi i x} dx > 0.
\]

Hence, by Lemma 4, \( aV \) is not u.d. \( \text{mod } 1 \).

Suppose, now, that \( x = 1/n \), \( n \) a positive integer. The sequence \( aS \) takes on the values \( 0, 1/n, \ldots, (n-1)/n \) \( \text{mod } 1 \) with equal frequency and the sequence \( aU \) is u.d. in \([0, 1/n]\). From this it is easy to see that \( aV \) is u.d. \( \text{mod } 1 \), and hence \( qV \) is u.d. \( \text{mod } 1 \) if \( q \in Q \setminus \{0\} \).

**References**


On the distribution of $\arg L(s, \chi)$ in the half-plane $\sigma > \frac{1}{2}$

by

P. D. T. A. ELLIOTT (Nottingham)

1. Introduction. For each complex number $s = \sigma + it$, $\sigma = \text{Re} s$, and non-principal Dirichlet character $\chi (\mod D)$, we consider the $L$-series which is defined to be the analytic continuation of

$$L(s, \chi_D) = \sum_{n=1}^{\infty} \chi(n) n^{-s} \quad (\sigma > 1).$$

For each real number $Q \geq 2$ let $M_Q$ denote the sum $\sum (p - 1)$ taken over all the odd prime numbers not exceeding $Q$. We thus count the total number of non-principal characters to prime moduli not exceeding $Q$. It follows from the prime number theorem that

$$M_Q = \frac{Q^\theta}{2\log Q} + O\left(\frac{Q^\theta}{\log^2 Q}\right).$$

When $L(s, \chi) \neq 0$, $\frac{1}{2} < \sigma \leq 1$, let $\arg L(s, \chi)$ denote a value of the argument of $L(s, \chi)$ defined by continuous displacement from the point $s = 2$ along an arc on which $L(s, \chi)$ does not vanish. Thus $\arg L(s, \chi)$ is only defined to within the addition of an integer multiple of $2\pi$. We set

$$\nu_Q \left(\frac{1}{2\pi} \arg L(s, \chi) \equiv \alpha (\mod 1)\right) = M_Q^{-1} \sum_{\nu \leq \alpha} \sum_\chi 1,$$

where the double sum counts those pairs $(\nu, \chi)$, with $\chi$ a non-principal character $(\mod D)$, and $p$ an odd prime not exceeding $Q$, for which $\arg L(s, \chi)$ is defined and has the value $2\pi(n + \alpha)$, $\alpha$ an integer, $0 \leq \alpha \leq \pi$.

In order to make the assertion in the following theorem meaningful we recall a few notions concerning distribution functions $(\mod 1)$.

A function $G(z)$ is said to be a distribution function $(\mod 1)$ if and only if it satisfies the following three conditions

(i) It increases in the wide sense.

(ii) It is right continuous, that is $G(z +) = G(z)$ for all $z$.

(iii) $G(z) = 1$ if $z \geq 1$, and $= 0$ if $z < 0$. 

4 — Acta Arithmetica XX.:1