ACTA ARITHMETICA
XX (1972)

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).

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 $\Lambda = (\lambda_k)$ of real numbers such that $\Lambda x = (\lambda_k x)$ is u.d. mod 1 if and only if $x \in M$. A normal set M must obviously satisfy

(i) $0 \notin M$,

(ii) $x \in M$, $n \in Z \setminus \{0\} \to nx \in M$

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

Additionally, if we require the sequence Λ 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 μ = 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.

---

(1) G. Rauzy has obtained a complete characterization of normal sets by different methods; see Bull. Soc. Math. France 98 (1971), pp. 401–414.

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

$$\lim_{N\to\infty} \frac{1}{N} \text{ (number of } \lambda_k \in J,\ 1 \leqslant k \leqslant N) = \|J\|/\|I\|,$$

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

We shall need the following lemmas:

LEMMA 1. (i) *If U is u.d.* mod 1, $k \in Z\setminus\{0\}$, *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 α, β are real numbers such that $1, \alpha, \beta$ are linearly independent over Q then the sequence $(n(\alpha, \beta))$ is w.d.* mod 1.

(iii) *Under the conditions of* (ii), *if* $0 \leqslant a < b \leqslant 1$ *and* (n_k) *is the increasing sequence of all positive integers n for which* $n\alpha \in [a, b]$ mod 1, *then* $(n_k\beta)$ *is w.d.* mod 1.

(iv) *If U is u.d. in $[0, a]$ and r is a real number then the sequence rU has a distribution function* mod 1, *and rU is u.d.* mod 1 $\leftrightarrow$ $ra \in Z\setminus\{0\}$. *If U is w.d. in $[0, a]$ then rU is d.w.* mod 1 *unless* $ra \in Z\setminus\{0\}$. *Similarly, if $\{U\}$ is w.d. in $[0, a]$ and if l is an integer, then lU is w.d.* mod 1 *if and only if* $la \in Z\setminus\{0\}$.

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 $Z\setminus\{0\}$ is a normal set: If Λ is u.d. in $[0, 1]$, then $x\Lambda$ is u.d. mod. 1 $\leftrightarrow x \in Z\setminus\{0\}$.

LEMMA 2. *Let $\Lambda_1, \Lambda_2, \ldots$ be disjoint, increasing sequences of real numbers and let $\Lambda = (\lambda_k)$ be an increasing sequence such that each λ_k belongs to some Λ_i,*

$$\lim \frac{1}{N} \text{ (number of } \lambda_k \text{ in } \Lambda_i,\ 1 \leqslant k \leqslant N) = n_i \quad (i = 1, 2, \ldots)$$

where $n_i > 0$, $\sum n_i = 1$, *and such that the terms of Λ belonging to Λ_i consists of segments of Λ_i of lengths tending to ∞.* (*Note that if* $\lim \Lambda_i = \infty$ *for each i then it is possible to construct such a Λ.*) *Then*

(i) *If each Λ_i is w.d.* mod. 1 *then Λ is u.d.* mod. 1.

(ii) *If some Λ_j is d.w.* mod 1 *and the other Λ_i are w.d.* mod 1 *then Λ 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* $QM + Q = M$. *Then*

(i) *There exists a strictly increasing sequence of integers Λ such that $x\Lambda$ is u.d.* mod 1 $\leftrightarrow x \notin M$.

(ii) *For each $\varepsilon > 0$ there exists a sequence Λ, where $|\lambda_k - k| < \varepsilon$, such that $x\Lambda$ is u.d.* mod 1 $\leftrightarrow x \notin M$.

In particular, if $M = R\setminus V$, 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 $S = \{s_i\} \subseteq M\setminus Q$ 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 $\Lambda = (n)$). For each i let $\bar{\Lambda}_i$ be the sequence of positive integers n, in increasing order, for which $ns_i \in [0, a]$(mod 1). Choose subsequences Λ_i of $\bar{\Lambda}_i$ such that the sequences Λ_i and Λ_j have no elements in common for $i \neq j$ and such that Λ_i is composed of segments of $\bar{\Lambda}_i$ of lengths tending to ∞. Finally, choose Λ to satisfy the hypotheses of Lemma 2. We claim that $x\Lambda$ is u.d. mod 1 $\leftrightarrow x \notin M$.

First, suppose $x \in M$. If x is rational then $x\Lambda$ is certainly not u.d. mod 1 since Λ is a sequence of integers. Suppose, then, that x is irrational and Λx is u.d. mod 1. Then $x = ps_i + q$ for some integer i and rational p, q. Because of Lemma 1 (i), $(kx)\Lambda$ is u.d. mod 1 for every $k \in Z\setminus\{0\}$, whence there exists $y = ls_i$, $l \in Z\setminus\{0\}$, such that $y\Lambda$ is u.d. mod 1. By Lemma 1 (iii) the sequence $y\bar{\Lambda}_j$ is w.d. mod 1 for $j \neq i$, so that $y\Lambda_j$ is w.d. mod 1 if $j \neq i$. However, $s_i\bar{\Lambda}_i \subseteq [0, a]$ (mod 1) and, in fact, the sequence $\{\bar{\Lambda}_i s_i\}$ is w.d. in $[0, a]$ ($\{\beta\}$ = fractional part of β). It follows that the same is true for $s_i\Lambda_i$ and thus, by Lemma 1 (iv) the sequence $y\Lambda_i$ is d.w. It follows from Lemma 2 (ii) that $y\Lambda$ is not u.d. mod 1, a contradiction.

Now, suppose $x \notin M$. 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 $x\Lambda_i$ is w.d. mod 1. Lemma 2 (i) shows that $x\Lambda$ 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 $\bar{\Lambda}_i$ as follows: Let k be a fixed integer $> 1/\varepsilon$ and let $a_i = 1 - s_i/k$. For each i let $\bar{\Lambda}_i = (\lambda_n)$ be the sequence chosen as follows:

$$\lambda_n = \begin{cases} n & \text{if } ns_i \in [0, a_i] \text{ mod } 1, \\ n + 1/k & \text{if } ns_i \in (a_i, 1) \text{ mod } 1. \end{cases}$$

The details will be omitted.

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

PROPOSITION 2. *Let $M \subseteq R$ 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 Λ_i be the sequence $\big(n(1/s_i)\big)$. Then $x\Lambda_i$ is w.d. mod 1 $\leftrightarrow x$ is not a rational multiple of s_i. If x is a rational multiple of s_i then $x\Lambda_i$ is d.w. We can now finish the proof by forming Λ 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 $M \subseteq Z$ be such that*

(i) $0 \notin M$,

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

Then there exists a sequence $U = (u_k)$ such that rU is u.d. mod 1 $\leftrightarrow r \in M$. *Furthermore, if $r \notin M$ then*

$$\limsup_{p\to\infty} \left| \frac{1}{p} \sum_{k=1}^{p} e^{2\pi i r u_k} \right| > 0.$$

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

$$f(x) = 1 + \frac{1}{2} \sum_{\substack{n \notin M \\ n \neq 0}} \frac{1}{2^n} e^{2\pi i n x}.$$

We may also write

$$f(x) = 1 + \frac{1}{2} \sum_{\substack{n \notin M \\ n \neq 0}} \frac{1}{2^n} \cos 2\pi n x$$

because of the symmetry of M. Thus we see that $f > 0$ on $[0,1]$. Let ν be the regular Borel probability measure on $[0,1]$ defined by $d\nu = f d\mu$. We observe that the nth Fourier coefficient of ν, $\hat{\nu}(n)$, is $0 \leftrightarrow n \in M$. Since $[0,1]$ is a compact metric space and ν is a probability measure on $[0,1]$, there exists a sequence V in $[0,1]$ such that V is ν-u.d., i.e., for every continuous function g on $[0,1]$ we have

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

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

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

But, by (*), $L(p) = \hat{\nu}(-pn)$ and this vanishes for all positive $p \leftrightarrow n \in M$.

Now, let $W = (w_k)$ be a sequence which is w.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

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

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

$$\lim_{N_j} \left| \frac{1}{N_j} \sum_{1}^{N_j} e^{2\pi i r u_k} \right| > 0 \quad \text{for} \quad r \in Z \setminus M$$

when N_j runs through the sequence (n_{2k}) and for $r \in R \setminus Z$ when N_j runs through the sequence (n_{2k+1}).

DEFINITION. Let $U_1, \ldots, U_k$ be sequences, say $U_i = (u_n^{(i)})$. The sequence $U = U_1 \otimes \ldots \otimes U_k$ 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

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

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 $U = U_1 \otimes \ldots \otimes U_k$ is u.d.* mod 1. *On the other hand, if there exists a strictly increasing sequence of integers (N_r) such that*

$$\lim_{r\to\infty} \left| \frac{1}{N_r} \sum_{k=1}^{N_r} e^{2\pi i u_k^{(j)}} \right| > 0 \qquad (j = 1, \ldots, k)$$

then U is not u.d. mod 1.

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

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

But

$$\frac{1}{N^k}\sum_{p=1}^{N^k} e^{2\pi i u_p n} = \left(\frac{1}{N}\sum_{p=1}^{N} e^{2\pi i n u_p^{(1)}}\right)\cdots\left(\frac{1}{N}\sum_{p=1}^{N} e^{2\pi i n u_p^{(k)}}\right)$$

so the result follows.

THEOREM 3. *Let* $S_1, \ldots, S_k$ *be subsets of* $Z\setminus\{0\}$ *such that* $nS_i \subseteq S_i$ *if* $n \in Z\setminus\{0\}$. *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 $V_i = (v_n^{(i)})$ and $W_i = (w_n^{(i)})$ 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 $t_0, \ldots, t_{2^k-1}$ be the 2^k k-tuples of 0's and 1's and let $t_j^{(i)}$ = the ith coordinate of t_j. Define the sequences U_i $(i = 1, \ldots, k)$ as follows:

$$U_i = (u_n^{(i)}),$$

where if $n_r \leqslant n = n_r + p < n_{r+1}$, $r \equiv s \pmod{2^k}$, $0 \leqslant s \leqslant 2^k - 1$, then

$$u_n^{(i)} = \begin{cases} \left(\frac{1}{a_i}\right) v_p^{(i)} & \text{if} \quad t_s^{(i)} = 0, \\ \left(\frac{1}{a_i}\right) w_p^{(i)} & \text{if} \quad t_s^{(i)} = 1. \end{cases}$$

We observe that xU_i is u.d. mod 1 if $x \in a_i S_i$. Let $U = U_1 \otimes \ldots \otimes U_k$. The observations made above and the first part of Lemma 4 show that xU is u.d. mod 1 if $x \in \bigcup a_i S_i$. Suppose $x \notin \bigcup a_i S_i$. Let l be the integer, $1 \leqslant l \leqslant 2^k$, so that for every i for which $1 \leqslant i \leqslant k$

$$t_{l-1}^{(i)} = \begin{cases} 0 & \text{if} \quad x = na_i,\ \text{some } n \in Z, \\ 1 & \text{if} \quad x \neq na_i. \end{cases}$$

From the choice of l it follows that for each i

$$\lim_{\substack{r\to\infty \\ r \equiv l \pmod{2^k}}} \frac{1}{n_r}\left|\sum_{p=1}^{n_r} e^{2\pi i x u_p^{(i)}}\right| > 0.$$

Therefore, by Lemma 4, xU is not u.d. 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*

$$(**) \qquad |x - k/p| < 1/(p^{1+d})$$

has infinitely many solutions for k *an integer,* p *a prime.*

Proof. This follows from the theorem on page 177 of [7] upon taking $r = q = N_j^{1/2}$, $\beta = N^{-1/5+\varepsilon}$. (This in fact shows that we may take $d = 1/5 - \varepsilon$, for any positive ε.) 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 $k_p = [p^{d/2}]$ and let B_p be the finite sequence $p, 2p, \ldots, k_p p$. Let (n_p) be a sequence of integers so that

$$n_p/(n_2 + \ldots + n_p) \to 1$$

and let S be the sequence

$$B_2, B_2, \ldots, B_p, B_p, \ldots, B_p, \ldots$$

where B_p occurs n_p times. Let U be any sequence u.d. in $[0, 1]$. Let $V = S \otimes U$. We claim that xV is u.d. mod 1 $\leftrightarrow x \in Q\setminus\{0\}$.

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

$$\limsup_{N\to\infty}\left|\sum_{r=1}^{N} e^{2\pi i x s_r}\right| = 1.$$

Furthermore, since U is u.d. in $[0, 1]$

$$\lim_{N\to\infty} \frac{1}{N}\left|\sum_{r=1}^{N} e^{2\pi i x u_r}\right| = \left|\int_0^x e^{2\pi i z}\,dz\right| > 0.$$

Hence, by Lemma 4, xV is not u.d. mod 1.

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

References

[1] J. Cigler and G. Helmberg, *Neuere Entwicklungen der Theorie der Gleichverteilung*, Jahr. der Deutsch. Math. Ver. 64-1 (1961), pp. 1–50.

[2] A. O. Gelfond and Ju. V. Linnik, *Elementary Methods in Analytic Number Theory*, 1965 (see chapter 7).

[3] M. Mendès-France, *Deux remarques concernant l'equirepartition des suites*, Acta Arith. 14 (1968), pp. 163–167.

[4] M. Mendès-France, *Nombres transcendants et ensembles normaux*, Acta Arith. 15 (1969), pp. 189–192.
[5] Y. Meyer, *Nombres de Pisot, Nombres de Salem et Analyse Harmonique*, Springer-Verlag Lecture Notes in Math. # 117.
[6] I. M. Vinogradov, *An elementary proof of a theorem of prime number theory* (in Russian), Izv. Akad. Nauk SSSR, Ser. Mat., 17 (1953), pp. 3–12.
[7] — *The Method of Trigonometric Sums in Number Theory*, Interscience Publishers.

Received on 28. 8. 1970 (115)

ACTA ARITHMETICA
XX (1972)

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 $s = \sigma+it$, $\sigma = \operatorname{Re} s$, and non-principal Dirichlet character $\chi \pmod D$, 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 $Q \geqslant 2$ 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

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

When $L(s,\chi) \neq 0$, $\frac{1}{2} < \sigma \leqslant 1$, 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 2π. We set

$$\nu_Q\left(\frac{1}{2\pi}\arg L(s,\chi) \leqslant z \pmod 1\right) = M_Q^{-1} \sum_{p\leqslant Q} \sum_{\chi\neq\chi_0} 1$$

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

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 $z \geqslant 1$, and $= 0$ if $z < 0$.