J. Austral. Math. Soc. (Series A) **49** (1990), 264–272

NOTES ON UNIFORM DISTRIBUTION MODULO ONE

G. MYERSON and A. D. POLLINGTON

Communicated by J. H. Loxton

Abstract

We exhibit a sequence (u_n) which is not uniformly distributed modulo one even though for each fixed integer $k \geq 2$ the sequence (ku_n) is u.d. (mod 1). Within the set of all such sequences, we characterize those with a well-behaved asymptotic distribution function. We exhibit a sequence (u_n) which is u.d. (mod 1) even though no subsequence of the form (u_{kn+j}) is u.d. (mod 1) for any $k \geq 2$. We prove that, if the subsequences (u_{kn}) are u.d. (mod 1) for all squarefree k which are products of primes in a fixed set $\mathscr{P}$, then (u_n) is u.d. (mod 1) if the sum of the reciprocals of the primes in $\mathscr{P}$ diverges. We show that this result is the best possible of its type.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 11 K 06.

1. Introduction

We recall the rudiments of the theory of sequences uniformly distributed modulo one (hereinafter abbreviated as u.d. (mod 1)). The standard reference for this material is [1].

By $\{x\}$ we mean the fractional part of x (we use the same notation for sets, but context should make the meaning clear). A sequence $(u_n) = (u_1, u_2, \ldots)$ of real numbers is said to be u.d. (mod 1) if

$$\lim_{N\to\infty} \frac{1}{N}\#\{n \leq N : \alpha \leq \{u_n\} < \beta\} = \beta - \alpha$$

for all α, β with $0 \leq \alpha < \beta \leq 1$. Writing $e(x)$ for $e^{2\pi i x}$ we can state the Weyl criterion as follows.

This research was supported by the Australian Research Council, grant #8515178.

THEOREM 1. *The sequence* (u_n) *is u.d.* (mod 1) *if and only if*

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

for all non-zero integers h.

We conclude our review with some immediate consequences of the Weyl criterion.

COROLLARY 1. *If* (u_n) *is u.d.* (mod 1) *then so is* (ku_n) *for any non-zero integer k.*

COROLLARY 2. *If for fixed* $k \geq 1$ *and for all* j, $1 \leq j \leq k$, *the sequence* (u_{kn+j}) *is u.d.* (mod 1) *then* (u_n) *is u.d.* (mod 1).

2. Multiples

In this section we first show by example that even a very weak converse of Corollary 1 is false.

THEOREM 2. *There exists a sequence* (u_n) , *not u.d.* (mod 1), *such that* (ku_n) *is u.d.* (mod 1) *for all integers* $k \geq 2$.

PROOF. Let $g(x) = x + \frac{1}{2\pi}\sin 2\pi x$. Note that g is a continuous, increasing function on $[0, 1]$, $g(0) = 0$, and $g(1) = 1$. Thus g has an inverse, h, with these same properties. Let (x_n) be any sequence u.d. (mod 1), and let $u_n = h(\{x_n\})$, $n = 1, 2, \ldots$. We claim that (u_n) satisfies the conditions of the theorem.

For any sequence (v_n), and for $0 \leq \alpha < \beta \leq 1$, let us write $\mathrm{pr}(\alpha \leq v < \beta)$ for

$$\lim_{N\to\infty}\frac{1}{N}\#\{n \leq N : \alpha \leq v_n < \beta\},$$

if the limit exists. Then

$$\begin{aligned}\mathrm{pr}(\alpha \leq u < \beta) &= \mathrm{pr}(\alpha \leq h(\{x\}) < \beta)\\ &= \mathrm{pr}(g(\alpha) \leq \{x\} < g(\beta)) = g(\beta) - g(\alpha)\end{aligned}$$

since x_n is u.d. (mod 1). But $g(\beta) - g(\alpha) = \beta - \alpha + \frac{1}{2\pi}(\sin 2\pi\beta - \sin 2\pi\alpha)$ which is, in general, not equal to $\beta - \alpha$, so (u_n) is not u.d. (mod 1).

Now let k be any integer greater than 1. Then

$$\begin{aligned}
\operatorname{pr}(\alpha \le \{ku\} < \beta) &= \operatorname{pr}(\alpha \le \{kh(x)\} < \beta) \\
&= \sum_{r=0}^{k-1} \operatorname{pr}(\alpha + r \le kh(x) < \beta + r) \\
&= \sum_{r=0}^{k-1} \operatorname{pr}\left(\frac{\alpha + r}{k} \le h(x) < \frac{\beta + r}{k}\right) \\
&= \sum_{r=0}^{k-1} \operatorname{pr}\left(g\left(\frac{\alpha + r}{k}\right) \le x < g\left(\frac{\beta + r}{k}\right)\right) \\
&= \sum_{r} \left(g\left(\frac{\beta + r}{k}\right) - g\left(\frac{\alpha + r}{k}\right)\right) \\
&= \beta - \alpha + \frac{1}{2\pi}\sum_{r}\left(\sin 2\pi\left(\frac{\beta + r}{k}\right) - \sin 2\pi\left(\frac{\alpha + r}{k}\right)\right) \\
&= \beta - \alpha
\end{aligned}$$

since $\sum_{r=0}^{k-1} \sin 2\pi(z + r/k) = 0$ for all real z and $k = 2, 3, \ldots$.

We now show that all the "nice" examples of sequences with the property given in Theorem 2 are essentially those produced in the proof of that theorem.

THEOREM 3. *Suppose* (ku_n) *is u.d.* (mod 1) *for* $k = 2, 3, \ldots,$ *and* $g(x) = \operatorname{pr}(0 \le \{u\} < x)$ *exists and is continuous. Then*

$$g(x) = x + c_1(1 - \cos 2\pi x) + c_2 \sin 2\pi x$$

for some constants c_1, c_2, *and, if* $x_n = g(u_n)$, *then* (x_n) *is u.d.* (mod 1).

REMARK. In an earlier version of this paper the conclusion of this theorem rested on the stronger hypothesis that g be differentiable. We thank Boping Jin for showing us how to weaken the hypothesis.

PROOF. By hypothesis we have, for $k = 2, 3, \ldots$, and $0 \le \alpha < \beta \le 1$,

$$\begin{aligned}
\beta - \alpha &= \operatorname{pr}(\alpha \le \{ku\} < \beta) \\
&= \sum_{r=0}^{k-1} \operatorname{pr}(\alpha + r \le k\{u\} < \beta + r) \\
&= \sum_{r=0}^{k-1} \operatorname{pr}\left(\frac{\alpha + r}{k} \le \{u\} < \frac{\beta + r}{k}\right) \\
&= \sum_{r} \left(g\left(\frac{\beta + r}{k}\right) - g\left(\frac{\alpha + r}{k}\right)\right).
\end{aligned}$$

Let $\alpha = 0$, $\beta = x$; then $\sum_r g((x+r)/k) - x = \sum_r g(r/k)$, a constant. Thus for $m \geq 1$ we have

$$\int_0^1 e(-mx) \sum_r g\left(\frac{x+r}{k}\right) dx = \int_0^1 xe(-mx)\, dx.$$

The right side of this equation is simply $-i/2\pi m$. Call the left side a_m; we get

$$\begin{aligned} a_m &= \sum_{r=0}^{k-1} \int_0^1 e(-mx) g\left(\frac{x+r}{k}\right) dx \\ &= \sum_r k \int_{r/k}^{(r+1)/k} e(-m(ky-r)) g(y)\, dy \\ &= k \int_0^1 e(-mky) g(y)\, dy. \end{aligned}$$

Thus,

$$\int_0^1 e(-ny) g(y)\, dy = -\frac{i}{2\pi n} \quad \text{for } n = k, 2k, \ldots.$$

But $k = 2, 3, \ldots$, so

$$\int_0^1 e(-ny) g(y)\, dy = -\frac{i}{2\pi n} \quad \text{for } n = 2, 3, \ldots.$$

Thus, the Fourier coefficients of $g(x)$ and of x are identical for $n \geq 2$, so

$$g(x) = x + c_1 + c_2 \sin 2\pi x + c_3 \cos 2\pi x$$

for some constants c_1, c_2, c_3. Since $g(0) = 0$ we have $c_1 + c_3 = 0$, and we have established the form of g.

Now let $x_n = g(u_n)$. Note that g is increasing, so $h = g^{-1}$ is defined. Then

$$\begin{aligned} \operatorname{pr}(\alpha \leq x < \beta) &= \operatorname{pr}(\alpha \leq g(u) < \beta) \\ &= \operatorname{pr}(h(\alpha) \leq u < h(\beta)) \\ &= g(h(\beta)) - g(h(\alpha)) = \beta - \alpha, \end{aligned}$$

so (x_n) is u.d. (mod 1).

3. Subsequences

In this section we first show by example that even a very weak converse of Corollary 2 is false. We use p only for primes, we write n (mod p) for the least non-negative residue of n modulo p, and we write $P(M)$ for $\prod_{p \leq M} p$.

https://doi.org/10.1017/S1446788700030548 Published online by Cambridge University Press

THEOREM 4. *The sequence* (u_n) *given by*

$$u_n = \sum_p^{\infty} \frac{n \pmod p}{P(p)},$$

is u.d. (mod 1) *, but for fixed* k, j, $k \geq 2$, *no subsequence of the form* u_{kn+j} *is u.d.* (mod 1).

Our proof uses some simple facts about the Cantor expansion of a real number. We collect these facts in a lemma.

LEMMA. *Every* α *in* $[0, 1)$ *has an expansion of the form*

$$\alpha = \sum_p^{\infty} \frac{\alpha_p}{P(p)}, \quad \text{where } \alpha_p \text{ are integers, } 0 \leq \alpha_p \leq p-1.$$

If we exclude expansions in which $\alpha_p = p - 1$ *for all* p *sufficiently large, the expansion is unique. The expansion of* α *terminates (that is,* $\alpha_p = 0$ *for all* p *sufficiently large) if and only if* $\alpha = c/P(M)$ *for some* M *and some integer* c, $0 \leq c < P(M)$. *Let*

$$\frac{c}{P(M)} = \sum_{p \leq M} \frac{\beta_p}{P(p)}, \quad 0 \leq \beta_p \leq p-1.$$

If p *is the largest prime not exceeding* M, *then* $c \equiv \beta_p \pmod p$; *if*

$$\frac{c}{P(M)} \leq \alpha < \frac{c+1}{P(M)},$$

then $\alpha_p = \beta_p$ *for* $p \leq M$.

PROOF OF THEOREM. We first prove that (u_n) is u.d. (mod 1). Given α and β with $0 \leq \alpha < \beta \leq 1$, and given $\varepsilon > 0$, let M be such that $P(M) > \varepsilon^{-1}$, let $a = [\alpha P(M)]$, and let $b = [\beta P(M)]$. Then

$$\begin{aligned}
\#\{n \leq N : \alpha \leq u_n < \beta\} &= \#\left\{n \leq N : \frac{a}{P(M)} \leq u_n < \frac{b+1}{P(M)}\right\} \\
&= \sum_{c=a}^{b} \#\left\{n \leq N : \frac{c}{P(M)} \leq u_n < \frac{c+1}{P(M)}\right\} \\
&= \sum_{c=a}^{b} \#\{n \leq N : n \equiv \beta_p(c) \pmod p,\ p \leq M\} \\
&\leq \sum_{c=a}^{b} \left(\frac{N}{P(M)} + 1\right) \\
&= (b-a+1)\frac{N}{P(M)} + b - a + 1,
\end{aligned}$$

where

$$\frac{c}{P(M)} = \sum_{p \le M} \frac{\beta_p(c)}{P(p)}.$$

Thus

$$\frac{1}{N}\#\{n \le N : \alpha \le u_n < \beta\} \le \beta - \alpha + 3\varepsilon$$

for N sufficiently large. A similar argument shows that

$$\frac{1}{N}\#\{n \le N : \alpha \le u_n < \beta\} \ge \beta - \alpha - 3\varepsilon$$

for N sufficiently large, whence (u_n) is u.d. (mod 1).

Now consider (u_{kn+j}), k and j fixed, $k \ge 2$, $n = 1, 2, \ldots$. Let p be any prime dividing k, so (u_{kn+j}) is a subsequence of (u_{pn+j}). Let j' be any integer with $j' \not\equiv j \pmod p$, and $0 \le j' < P(p)$. Then

$$\frac{j'}{P(p)} \le u_{pn+j} < \frac{j'+1}{P(p)}$$

is impossible, so

$$\frac{j'}{P(p)} \le u_{kn+j} < \frac{j'+1}{P(p)}$$

is impossible, and (u_{kn+j}) is not u.d. (mod 1).

Our final result can be seen as complementary to Corollary 2.

THEOREM 5. *Let $\mathscr{P}$ be a set of primes such that $\sum_{p\in\mathscr{P}} \frac{1}{p}$ diverges. Let $\mathscr{K}$ denote the set of squarefree integers divisible only by primes in $\mathscr{P}$. If (u_{kn}) is u.d.* (mod 1) *for every $k > 1$ in $\mathscr{K}$ then (u_n) is u.d.* (mod 1).

REMARK. If $\mathscr{P}$ is a set of primes such that $\sum_{p\in\mathscr{P}} \frac{1}{p}$ converges then given any irrational α the sequence (u_n) given by

$$u_n = \begin{cases} n\alpha, & \text{if } p|n \text{ for some } p \in \mathscr{P}, \\ 0, & \text{otherwise} \end{cases}$$

has the property that (u_{kn}) is u.d. (mod 1) for any k divisible by some prime in $\mathscr{P}$, but (u_n) is not u.d. (mod 1) since $u_n = 0$ on a set of positive density.

PROOF. We put

$$P(\mathscr{P}, M) = \prod_{\substack{p\in\mathscr{P} \\ p\le M}} p.$$

By the Weyl criterion, we have

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}e(mu_{kn})=0$$

for all non-zero integers m and all $k\in\mathscr{K}$, $k>1$. Thus given $M>0$ there is an $N_0=N_0(m, M)$ such that if $N>N_0$ then

$$\frac{k}{N}\left|\sum_{n=1}^{N/k}e(mu_{kn})\right|<\frac{1}{M} \tag{1}$$

for all $k|P(\mathscr{P}, M)$, $k>1$. Now

$$\begin{aligned}\frac{1}{N}\left|\sum_{n=1}^{N}e(mu_n)\right| &\le \frac{1}{N}\sum_{\substack{k|P(\mathscr{P}, M)\\ k>1}}|\mu(k)|\left|\sum_{n=1}^{N/k}e(mu_{kn})\right|+\frac{1}{N}\sum_{\substack{n\le N\\ (n, P(\mathscr{P}, M))=1}}1\\ &\le \frac{1}{M}\prod_{p|P(\mathscr{P}, M)}\left(1+\frac{1}{p}\right)+\prod_{p|P(\mathscr{P}, M)}\left(1-\frac{1}{p}\right)\end{aligned}$$

by (1). The first term on the right goes to 0 as M goes to infinity:

$$\begin{aligned}\prod_{p|P(\mathscr{P}, M)}\left(1+\frac{1}{p}\right) &\le \prod_{p\le M}\left(1+\frac{1}{p}\right)\\ &= \exp\sum_{p\le M}\log\left(1+\frac{1}{p}\right)\le \exp\sum_{p\le M}\frac{1}{p}=O(\log M).\end{aligned}$$

Since $\sum_{p\in\mathscr{P}}\frac{1}{p}$ diverges, the second term on the right also goes to zero as M goes to infinity. Hence, (u_n) is u.d. (mod 1), by Weyl's criterion.

4. Multiples in higher dimensions

We conclude with a discussion of uniform distribution in higher dimensions, where the statement analogous to Theorem 2 goes badly wrong. A sequence $(\mathbf{u}_n)$ of real m-tuples is said to be u.d. (mod 1) if

$$\lim_{N\to\infty}\frac{1}{N}\#\{n\le N:\boldsymbol{\alpha}\le\mathbf{u}_n<\boldsymbol{\beta}\}=|\boldsymbol{\beta}-\boldsymbol{\alpha}|$$

for all $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ with $\mathbf{0}\le\boldsymbol{\alpha}<\boldsymbol{\beta}\le\mathbf{1}$; here, and below, $(\mathbf{u}_n)$ means $(\{u_n^{(1)}\}, \dots, \{u_n^{(m)}\})$; $(x_1, \dots, x_m)<(y_1, \dots, y_m)$ means $x_j<y_j$ for $j=1, \dots, m$; $|(x_1, \dots, x_m)|$ means $x_1x_2\cdots x_m$; $\mathbf{0}$ means $(0, \dots, 0)$, and $\mathbf{1}$ means $(1, \dots, 1)$. The Weyl criterion is

THEOREM $1'$. *The sequence* $(\mathbf{u}_n)$ *is u.d.* (mod 1) *if and only if*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}e(\mathbf{h}\cdot\mathbf{u}_n)=0$$

for all non-zero integer m*-tuples* $\mathbf{h}$.

An immediate consequence is

COROLLARY $1'$. *If* $(\mathbf{u}_n)$ *is u.d.* (mod 1) *then so is* $(A\mathbf{u}_n)$ *for any non-singular integer matrix* A.

Another simple consequence is

COROLLARY 3. *If* A *is an integer matrix with determinant* ± 1 *and* $(A\mathbf{u}_n)$ *is u.d.* (mod 1) *then* $(\mathbf{u}_n)$ *is u.d.* (mod 1).

PROOF. Under the hypotheses, A^{-1} has integer entries, so, by the previous corollary, $(A^{-1}A\mathbf{u}_n)$ is u.d. (mod 1).

A statement analogous to Theorem 2 would be, "there exists a sequence $(\mathbf{u}_n)$, not u.d. (mod 1), such that $(A\mathbf{u}_n)$ is u.d. (mod 1) for all integer matrices A with $\det A \geq 2$." However, this statement is far from being true. Instead we have

THEOREM 6. *Let* S *be a set of* $m\times m$ *integer matrices, and suppose that for every integer row* m*-vector* $\mathbf{h}$ *there exists a matrix* A *in* S *and an integer row* m*-vector* $\mathbf{k}$ *such that* $\mathbf{k}A=\mathbf{h}$. *Then if* $(A\mathbf{u}_n)$ *is u.d.* (mod 1) *for all* A *in* S, *then* $(\mathbf{u}_n)$ *is u.d.* (mod 1).

PROOF. Given a non-zero integer m-tuple $\mathbf{h}$, considered as a row vector, let A in S and $\mathbf{k}$ an integer row-vector be such that $\mathbf{k}A=\mathbf{h}$. Then

$$\sum_{n=1}^{N}e(\mathbf{h}\cdot\mathbf{u}_n)=\sum_{n}e(\mathbf{k}A\cdot\mathbf{u}_n)=\sum_{n}e(\mathbf{k}\cdot A\mathbf{u}_n)=o(N),$$

since $(A\mathbf{u}_n)$ is u.d. (mod 1). Thus, $(\mathbf{u}_n)$ is u.d. (mod 1).

EXAMPLE. Let $m=2$. One easily verifies that

$$S=\left\{\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}1&-1\\1&1\end{pmatrix}\right\}$$

has the property required. If c is even, then $(c\quad d)=(c/2\quad d)\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)$; if d is even, then $(c\ d)=(c\ d/2)\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$; if c and d are both odd (or both even),

https://doi.org/10.1017/S1446788700030548 Published online by Cambridge University Press

then $(c\ d) = ((c-d)/2\ (c+d)/2)\binom{1\ -1}{1\ \ 1}$. Thus if $(A\mathbf{u}_n)$ is u.d. (mod 1) for all A in S, then $(\mathbf{u}_n)$ is u.d. (mod 1).

Note added in proof

Peter Sarnak has pointed out that Theorem 3 holds under the weaker hypothesis that $g(x)$ exists as a measure. Also, Michel Mendès France has pointed out to us that Theorem 2 is a special case of the main theorem of F. Dress and M. Mendès France, 'Caractérisation des ensembles normaux dans $\mathbf{Z}$,' *Acta Arith.* **17** (1970), 115–120.

References

[1] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, (Wiley, 1974).

School of Mathematics, Physics,
Computing and Electronics
Macquarie University
Australia 2109

Department of Mathematics
Brigham Young University
Provo, Utah 84602
U.S.A.