141. On the Uniform Distribution of Sequences of Integers

By Saburô UCHIYAMA

Department of Mathematics, Hokkaidô University, Sapporo

(Comm. by Z. SUETUNA, M.J.A., Dec. 12, 1961)

1. Introduction. Consider an infinite sequence $A=(a_n)$ of integers. For any integers j and $m\geqq 2$ we denote by $A(N,j,m)$ the number of terms a_n $(1\leqq n\leqq N)$ satisfying the condition $a_n\equiv j \pmod m$. The sequence A is said to be *uniformly distributed modulo* m if the limit

$$\lim_{N\to\infty}\frac{1}{N}A(N,j,m)=\frac{1}{m}$$

exists for all j, $1\leqq j\leqq m$. If A is uniformly distributed modulo m for every integer $m\geqq 2$, we say simply that A is *uniformly distributed.*

I. Niven [1] has exhibited a number of interesting properties of uniformly distributed sequences of integers. Among others he proved that the sequence A, defined by $a_n=[ns]$, is uniformly distributed if and only if s is irrational or $s=1/k$ for some non-zero integer k, and that the uniform distribution of the sequence $([ns])$ for every irrational s is equivalent to the well-known theorem that the sequence of the fractional parts of ns is uniformly distributed modulo 1 for every irrational s (cf. e.g. [2]). It is not difficult to show that, for every infinite sequence (a_n) of mutually distinct integers, the sequence $([a_n s])$ is uniformly distributed for almost all real numbers s. (Here 'almost all' means 'all but a set of Lebesgue measure zero'.)

The main purpose of the present note is to obtain some criteria for sequences of integers to be uniformly distributed (with or without the reference to modulus m).

Let us put, for brevity's sake,

$$e(x)=\exp(2\pi ix).$$

We shall prove:

Theorem 1. *Let $A=(a_n)$ be an infinite sequence of integers. A necessary and sufficient condition that A be uniformly distributed modulo m, where $m\geqq 2$, is that*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}e\left(a_n\frac{h}{m}\right)=0 \tag{1}$$

for all $h=1,2,\cdots,m-1$.

Hence:

Corollary. *A necessary and sufficient condition that an infinite sequence $A=(a_n)$ of integers be uniformly distributed is that*

(2)
$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}e(a_n t)=0$$
for all rational numbers $t, t\not\equiv 0 \pmod 1$.

It is of some interest to note that the Corollary to Theorem 1 is, in a sense, dual to the theorem of H. Weyl [2] stating that an infinite sequence of real numbers (α_n) is uniformly distributed modulo 1 if and only if
$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}e(\alpha_n t)=0$$
for all non-zero integers t.

2. Proof of Theorem 1. Suppose that the sequence $A=(a_n)$ is uniformly distributed modulo m, $m\geqq 2$. Then we have for $1\leqq h\leqq m-1$
$$\begin{aligned}\frac{1}{N}\sum_{n=1}^{N}e\left(a_n\frac{h}{m}\right)&=\frac{1}{N}\sum_{j=1}^{m}A(N,j,m)\,e\left(\frac{jh}{m}\right)\\&=\frac{1}{N}\sum_{j=1}^{m}\left(\frac{N}{m}+o(N)\right)e\left(\frac{jh}{m}\right)\\&=\sum_{j=1}^{m}o(1)\,e\left(\frac{jh}{m}\right)\\&=o(1)\qquad(N\to\infty).\end{aligned}$$

Conversely, suppose that
$$\frac{1}{N}\sum_{n=1}^{N}e\left(a_n\frac{h}{m}\right)=o(1)\qquad(N\to\infty)$$
for all $h=1,2,\cdots,m-1$. Then, it is clear that
$$\sum_{j=1}^{m}A(N,j,m)\,e\left(\frac{jh}{m}\right)=\begin{cases}o(N)\quad(N\to\infty)&\text{for } 1\leqq h\leqq m-1,\\ N&\text{for } h=m.\end{cases}$$
Now, let k be any integer satisfying $1\leqq k\leqq m$. It follows from the above relation that
$$\begin{aligned}mA(N,k,m)&=\sum_{j=1}^{m}A(N,j,m)\sum_{h=1}^{m}e\left(\frac{(j-k)h}{m}\right)\\&=\sum_{h=1}^{m}e\left(-\frac{kh}{m}\right)\sum_{j=1}^{m}A(N,j,m)\,e\left(\frac{jh}{m}\right)\\&=o(N)+N\qquad(N\to\infty),\end{aligned}$$
whence
$$\frac{1}{N}A(N,k,m)=\frac{1}{m}+o(1)\qquad(N\to\infty).$$

This completes the proof of Theorem 1.

3. An illustration. As an application of the Corollary to Theorem 1 we shall prove the following

Theorem 2. *Let q be an integer greater than 1. Then the sequence $A=(a_n)$, defined by*
$$a_n=[n^{1/q}s],$$
is uniformly distributed for every non-zero real number s.

It suffices to prove this for s positive. Put

$$a=[s],\ b=[N^{1/q}s],$$

where $N\geqq 1$. For any integer k between a and b define $B(k)$ as the number of solutions in n of the equation

$$[n^{1/q}s]=k.$$

Then

$$B(k)=\left(\frac{k+1}{s}\right)^q-\left(\frac{k}{s}\right)^q+O(1)$$
$$=\frac{q}{s^q}k^{q-1}+O(k^{q-2}).$$

Now, for any real (not necessarily rational) number t with $t\not\equiv 0 \pmod 1$, we have

$$\frac{1}{N}\sum_{n=1}^{N}e(a_n t)=\frac{1}{N}\sum_{k=a}^{b}B(k)\,e(kt)$$
$$=\frac{1}{N}\sum_{k=a}^{b}\left(\frac{q}{s^q}k^{q-1}+O(k^{q-2})\right)e(kt)$$
$$=O(N^{-1/q})=o(1) \qquad (N\to\infty),$$

since

$$\sum_{k=a}^{b}k^{q-1}\,e(kt)=O(N^{(q-1)/q}),$$

which can be easily verified by induction on q, and

$$\sum_{k=a}^{b}O(k^{q-2})\,e(kt)=O(b\cdot b^{q-2})=O(N^{(q-1)/q}).$$

The result now follows from the Corollary to Theorem 1.

Note that Theorem 2 is not true for $q=1$.

4. An observation. It is known that, if (a_n) is an infinite sequence of mutually distinct integers, then the sequence $(a_n s)$ is uniformly distributed modulo 1 for almost all real numbers s (cf. [2]). We wish to show that the same is true for every uniformly distributed sequence (a_n) of integers. This means, in particular, that if a sequence (a_n) of integers is uniformly distributed then the condition (2) holds for almost all real numbers t.

Theorem 3. *Let $A=(a_n)$ be a uniformly distributed sequence of integers. Then the sequence $(a_n s)$ is uniformly distributed modulo 1 for almost all real numbers s.*

It is sufficient to prove Theorem 3 for s with $0<s<1$. Define $B(k)$ as the number of terms $a_n(1\leqq n\leqq N)$ which are equal to k, k being an integer. Clearly

$$A(N,j,m)=\sum_{k\equiv j \pmod m}B(k).$$

For any non-zero integer h we have

$$\int_0^1\left|\frac{1}{N}\sum_{n=1}^{N}e(ha_n t)\right|^2dt=\frac{1}{N^2}\int_0^1\left|\sum_k B(k)\,e(hkt)\right|^2dt$$
$$=\frac{1}{N^2}\sum_k B^2(k).$$

Given any real number $\varepsilon, 0<\varepsilon<1$, we choose an integer m such that

$$\frac{5}{\varepsilon}<m<\frac{25}{4\varepsilon}$$

and then take N so large as to satisfy

$$\left|\frac{A(N, j, m)}{N}-\frac{1}{m}\right|<\frac{\varepsilon}{5}$$

for all $j=1,2,\cdots, m$. This is possible since it is assumed that the sequence A is uniformly distributed, i.e. uniformly distributed modulo m for every integer $m\geqq 2$. We have then

$$\begin{aligned}\frac{1}{N^2}\sum_k B^2(k)&=\sum_{j=1}^m \frac{1}{N^2}\sum_{k\equiv j(\mathrm{mod}\ m)} B^2(k)\\ &\leqq \sum_{j=1}^m \frac{1}{N^2} A^2(N, j, m)\\ &<\sum_{j=1}^m\left(\frac{1}{m}+\frac{\varepsilon}{5}\right)^2\\ &<m\frac{4\varepsilon^2}{25}<\varepsilon.\end{aligned}$$

Thus we have for all sufficiently large N

$$\int_0^1\left|\frac{1}{N}\sum_{n=1}^N e(ha_n t)\right|^2 dt<\varepsilon.$$

Since $\varepsilon, 0<\varepsilon<1$, is arbitrary, it follows that

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

for almost all t with $0<t<1$. As a denumerable union of sets of measure zero is of measure zero, this completes the proof of Theorem 3, in view of the Weyl criterion quoted in the Introduction.

A direct consequence of Thorem 3 is that if a sequence (a_n) of integers is uniformly distributed then so is also the sequence $([a_n s])$ for almost all real numbers s.

The converse of Theorem 3 does not hold in general, as the following example shows. The sequence $(n^2 s)$ is known to be uniformly distributed modulo 1 for every irrational s, while the sequence (n^2) is not uniformly distributed modulo m for infinitely many m (cf. [1]): indeed, the congruence $n^2\equiv j \pmod m$ is solvable in n only for $(m+1)/2$ incongruent values of $j \pmod m$ for every odd prime m.

5. **Remarks.** Niven [1] has observed that if a sequence $A=(a_n)$ of integers is uniformly distributed modulo $m, m\geqq 2$, then we have

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^N e(a_n/m)=0 \tag{3}$$

(which is a special case of (1) with $h=1$), but the converse does not hold except for $m=2$ and $m=3$. Here, it should be noted that, when $m=2$ or $m=3$, the condition (3) is actually equivalent to the condition (1), as is readily seen. However, in general, (3) is so weaker than (1) that it is unable to guarantee the uniform distribution modulo m of the sequence A.

So far we have treated only the one dimensional distribution of integers on the real line. The notion of the uniform distribution (with or without the reference to modulus m) of sequences of integers can naturally be extended to higher dimensional spaces (considering the distribution of sequences of integral vectors or lattice points instead), and the corresponding extensions of the results of this note will be obtained in an appropriate way.

References

[1] I. Niven: Uniform distribution of sequences of integers, Trans. Amer. Math. Soc., **98**, 52-61 (1961).
[2] H. Weyl: Über die Gleichverteilung von Zahlen modulo Eins, Math. Ann., **77**, 313-352 (1916).