

## SOME NOTES ON UNIFORM DISTRIBUTION OF SEQUENCES OF INTEGERS

SHI-HAW CHENG

College of Engineering, National Chiao Tung University

(Received April 27, 1972)

**Abstract**—In this paper we discuss the distribution property of any geometric progression  $\{ar^n\}$  with  $a$  and  $r$  integers and we apply the result for the uniform distribution of sequences of real numbers mod 1.

### §1. INTRODUCTION

In 1961, I. Niven published a paper "Uniform distribution of sequence of integers."<sup>2</sup> He introduced the notion of uniform distribution mod  $m$ . Let  $\{a_n\}$  be a sequence of integers. Let  $m \geq 2$  be an integer. For an integer  $j$  and a natural number  $N$  we define  $A(j, N)$  to be the number of elements from  $a_1, a_2, \dots, a_N$  such that  $a_i \equiv j \pmod{m}$ . We say that the sequence  $\{a_n\}$  of integers is uniformly distributed mod  $m$  if

$$\lim_{N \rightarrow \infty} \frac{A(j, N)}{N} = \frac{1}{m} \text{ for } j=0, 1, 2, \dots, m-1$$

(or equivalently, for a complete system of residues mod  $m$ ).

As an example, Niven consider the sequence  $\{an+b\}$  with integers  $a$  and  $b$ ,  $n=1, 2, 3, \dots$ . He stated that any arithmetic progression  $\{an+b\}$ ,  $n=1, 2, 3, \dots$  is uniformly distributed mod  $m$  if and only if  $g, c, d(a, m)=1$ . But he did not give the proof. We shall give the complete proof in this note (see section 3).

It is naturally to ask that what is the distribution property of any geometric progression  $\{ar^n\}$  with  $a$  and  $r$  integer,  $n=1, 2, \dots$ . This is our main object in this note (see section 3). In section 2. We also give some lemmas which we shall need in our propose. Finally we shall give relationship between the uniform distribution of sequence of real numbers mod 1 and the uniform distribution of sequences of integers mod  $m$ .

### §2. SOME LEMMAS

LEMMA 1: If  $(a, m)=1$ , then  $ax \equiv b \pmod{m}$  has a solution.<sup>3</sup>

PROOF: By Euler's theorem, we have

$$a^{\phi(m)} \equiv 1 \pmod{m}, \text{ because } (a, m)=1$$

It follows from Euler's theorem, we obtain that

$$ba^{\phi(m)-1} \text{ is a solution of } ax \equiv b \pmod{m}$$

LEMMA 2: If  $(a, m)=1$ . then  $ax \equiv ay \pmod{m}$  if and only if  $x \equiv y \pmod{m}$ .<sup>1</sup>

PROOF: This follows from the definition of congruence.

LEMMA 3: If a sequence  $\{a_n\}$  is uniformly distributed mod  $m$ , then it is uniformly distributed mod  $m$ , then is uniformly distributed mod every positive division of  $m$ .

PROOF: Since  $\{a_n\}$  is uniformly distributed mod  $m$  we have

$$\lim_{N \rightarrow \infty} \frac{A(j, N)}{N} = \frac{1}{m} \text{ for } j=0, 1, 2 \dots m-1$$

Now let  $d|m \Rightarrow m = m_1 d$

consider  $A(i, n) = |\{1 \leq n \leq N | a_n \equiv i \pmod{d}\}|$

$$i=0, 1, 2, \dots, d-1$$

then

$$A(i, N) = m_1 A(j, N),$$

and

$$\lim_{N \rightarrow \infty} \frac{A(i, N)}{N} = m_1 \lim_{N \rightarrow \infty} \frac{A(j, N)}{N} = m_1 \frac{1}{m} = \frac{m_1}{m_1 d} = \frac{1}{d}$$

So that the sequence  $\{a_n\}$  is uniformly distributed mod  $d$ .

### §3. MAIN RESULTS

THEOREM 1: The sequence  $\{an+b\}$  is uniformly distributed mod  $m$  if and only if  $g, c, d (a, m) = 1$ .

PROOF: If  $(a, m) = d > 1$

then consider  $an+b \equiv b \pmod{d} \quad n=1, 2 \dots N$ .

$$\Leftrightarrow an \equiv 0 \pmod{d}$$

$$\Rightarrow A(b, N) = N$$

$$\Rightarrow \frac{A(b, N)}{N} = 1$$

$$\Rightarrow \lim_{N \rightarrow \infty} \frac{A(b, N)}{N} = 1 \neq \frac{1}{d}$$

i.e  $\{an+b\} \quad n=1, 2, \dots$  is not uniformly distributed mod  $d$ . By Lemma 3, we have  $\{an+b\} \quad n=1, 2, 3, \dots$  is not uniformly distributed mod  $m$ .

On the other hand, suppose  $(a, m) = 1$ . For an interger  $j, A(j, N)$  is number of solutions  $an+b \equiv j \pmod{m}, 1 \leq n \leq N$ .

Let us write  $N = gm+r, 0 \leq r < m$ . Whenever  $n$  runs through a complete residue system mod  $m$ , then  $an+b$  runs through a complet residue system mod  $m$ . Thus, by lemma 1, the congruence has at least  $g$  and at most  $g+1$  solutions

$$\Rightarrow \frac{g}{gm+r} \leq \frac{A(j, N)}{N} \leq \frac{g+1}{gm+r}$$

$$\Rightarrow \lim_{g \rightarrow \infty} \frac{g}{gm+r} \leq \lim_{N \rightarrow \infty} \frac{A(j, N)}{N} \leq \lim_{g \rightarrow \infty} \frac{g+1}{gm+r}$$

$$\Rightarrow \lim_{N \rightarrow \infty} \frac{A(j, N)}{N} = \frac{1}{m} \text{ for } j=0, 1, 2, \dots, m-1$$

DEFINITION: The sequence  $\{a_n\}$  of integers is called uniformly distributed if it is uniformly distributed mod  $m$  for all integers  $m \geq 2$ .

THEOREM 2: The sequence  $\{an+b\}$  is uniformly distributed if and only if  $a = \pm 1$ .

PROOF: This simply follows from theorem 1, and the fact that

$$(a, m) = 1 \text{ for all } m \geq 2, \text{ if and only if } a = \pm 1.$$

THEOREM 3: Let  $\{ar^n\}_{n=0, 1, 2, \dots}$  be a geometric progression of integers, then  $\{ar^n\}$  is not uniformly distributed mod  $m$  for all  $m \geq 2$ .

PROOF: We shall prove this theorem in two cases:

case 1. If  $(a, m) = d > 1$ , then

$$ar^n \equiv 0 \pmod{d} \text{ for all } n=0, 1, 2, \dots$$

This means that  $A(0, N) = N$ , and then

$$\lim_{N \rightarrow \infty} \frac{A(0, N)}{N} = 1 \neq \frac{1}{d}$$

Therefore the sequence  $\{ar^n\}_{n=0, 1, 2, \dots}$  is not uniformly distributed mod  $d$ . It follows from Lemma 3. that the sequence  $\{ar^n\}_{n=0, 1, 2, \dots}$  is not uniformly distributed mod  $m$  for all  $m \geq 2$ .

case 2. If  $(a, m) = 1$  then

consider  $ar^n \equiv j \pmod{m}$  for  $j=0, 1, 2, \dots, m-1$ , and consider the following two cases.

1° If  $(r, m) = d_1 > 1$

$$\Rightarrow ar^n \equiv 0 \pmod{d_1} \text{ for all } n=0, 1, 2, \dots$$

and then

$$\lim_{N \rightarrow \infty} \frac{A(0, N)}{N} = 1 \neq \frac{1}{d_1}$$

i.e the sequence  $\{ar^n\}_{n=0, 1, 2, \dots}$  is not uniformly distributed mod  $d_1$ .

Since  $d_1 | m$  and then by Lemma 3. we have

$\{ar^n\}_{n=0, 1, 2, \dots}$  is not uniformly distributed mod  $m$  for all  $m \geq 2$ .

2° If  $(r, m) = 1$ ,

then

$$(r^n, m) = 1 \text{ for all } n=0, 1, 2, \dots$$

and

$$(ar^n, m) = 1 \text{ for all } n=0, 1, 2, \dots$$

So that  $A(0, N) = 0$

$$\Rightarrow \lim_{N \rightarrow \infty} \frac{A(0, N)}{N} = 0 \neq \frac{1}{m}$$

Hence  $\{ar^n\} n=0, 1, 2, \dots$  is not uniformly distributed mod  $m$  for all  $m \geq 2$ . This completes the proof.

§4. APPLICATION

In this section, we wish to apply theorem 3. for the uniform distribution of sequences of real numbers mod 1.

First of all, we shall give the definition of uniform distribution of sequence of sequence of real number mod 1.

DEFINITION: Let  $\{X_n\}, n=1, 2, \dots$  be a sequence of real numbers in the unit interval, let  $M$  be a subset of unit internal. For a fixed natural number  $N$ , define  $A(M, N)$  be the number of  $X_n, 1 \leq n \leq N$ , which lie in  $M$ . The sequence  $\{X_n\}$  is called uniformly distributed in the unit interval if for every subinterval  $I = [\alpha, \beta]$  of the unit interval the following holds:

$$\lim_{N \rightarrow \infty} \frac{A(I, N)}{N} = \beta - \alpha.$$

DEFINITION: The sequence  $\{X_n\} n=1, 2, 3, \dots$  of real numbers is called uniformly distributed modulo 1 if the sequence of the fractional part  $\{(X_n)\}$  is uniformly distributed in the unit interval.

THEOREM 4. The sequence  $\{X_n\}$  is uniformly distributed mod 1, if and only if the sequence  $\{[mX_n]\}$  is uniformly distributed  $m$  for all integers  $m \geq 2$ .

PROOF: For fixed  $m \geq 2$  and  $j$  with  $0 \leq j \leq m-1$  we have

$$\begin{aligned} [mX_n] &\equiv j \pmod{m} \\ \Leftrightarrow mX_n &= Km + j \text{ for some intyer } K \\ \Leftrightarrow Km + j &\leq mX_n < Km + j + 1 \\ \Leftrightarrow K + \frac{j}{m} &\leq X_n < K + \frac{j+1}{m} \\ \Leftrightarrow \frac{j}{m} &\leq (X_n) < \frac{j+1}{m} \end{aligned}$$

thus

$$A(j, N) = A([\frac{j}{m}, \frac{j+1}{m}], N)$$

If  $\{X_n\}$  is uniformly distributed mod 1, then

$$\lim_{N \rightarrow \infty} \frac{A(j, N)}{N} = \lim_{N \rightarrow \infty} \frac{A([\frac{j}{m}, \frac{j+1}{m}], N)}{N} = \frac{1}{m} \text{ for all } j=0, 1, 2, \dots, m-1$$

$\Rightarrow [mX_n]$  is uniformly distributed mod  $m$ , for all  $m \geq 2$ .

On the other hand, if  $[mX_n]$  is uniformly distributed mod  $m$ , then

$$\lim_{N \rightarrow \infty} \frac{A([\frac{j}{m}, \frac{j+1}{m}], N)}{N} = \lim_{N \rightarrow \infty} \frac{A(j, N)}{N} = \frac{1}{m}$$

Letting  $m$  run through all the integers  $\geq 2$ , it follows that

$$\lim_{N \rightarrow \infty} \frac{A(I, N)}{N} = \lambda(I) \text{ where } \lambda(I) \text{ denote the length of } I$$

This holds for all subintervals  $I$  of the unit interval with rational endpoints. Using the usual approximation method, we have the above equation holds for all subintervals of the unit interval.

Now we have the following theorem:

**THEOREM 5.** For all integer  $m \geq 2$ , the sequence  $\left\{ \frac{ar^n}{m} \right\} n=0, 1, 2, \dots$  is not uniformly distributed mod 1.

**PROOF:** It simply follows from theorem 4 and theorem 3.

**REMARK:** Theorem 3. may be prove by using Niven-Uchiyama Criterion which stated as follows:

$\{X_n\}$  is uniformly distributed mod  $m$  if and only if

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N e^{2\pi i h/m a_n} = 0 \text{ for } h=1, 2, \dots, m-1$$

### ACKNOWLEDGEMENT

The author's greatest debt of gratitude is due professor Dr. Jau-Shyong Shiue, for his encouragement and advice.

### REFERENCES

1. T. Nagell, Introduction to number theory, New York John Wiley 1951, pp. 68-73.
2. IVAN NIVEN, Uniform distribution of sequence of integers, AMER. MATH Society Jan 1961, Vol 98, No. 1, pp. 52-61.
3. IVAN NIVEN, An introduction to the theory of numbers, New York Lowdon John Wiley 1960.
4. H. Weyl, Uber die Gleichverteilung Von Zahlen mod Eins, Math Ann 77 (1916), pp. 313-352.