数理解析研究所講究録
第537巻 1984年 1-10

WEAKLY UNIFORMLY DISTRIBUTED SEQUENCES OF INTEGERS

KENJI NAGASAKA

APPLICATIONS OF NUMBER THEORY TO NUMERICAL ANALYSIS
RESEARCH INSTITUTE OF MATHEMATICAL SCIENCES
KYOTO UNIVERSITY, 31.5-2.6(1984)

1. INTRODUCTION.

Number theory had long been considered as the pureset branch of pure mathematics, since many beautiful and powerful results have been needed to obtain only one theorem in number theory and its converse, i.e. applications of number theory to other mathematics, did take place quite rarely. These are probably the main reason to mention the queenliness of number theory.

Over twenty years ago, some of mathematicians started to investigate problems of diophantine analysis and uniform distribution of point sets from not only their intrinsic interests but also interests in their applications to numerical analysis. Together with the progress of digital computers, number theory is now applicable to mathematical sciences.

Applications of number theory seem to be made mainly through so-called Monte-Carlo simulation including numerical integration. Monte-Carlo method is a kind of heuristic device to solve various problems: When a certain difficulty arises to obtain an exact ana-

lytic formula, Monte-Carlo simulation gives practically sufficient numerical tables. To verify the validity for newly invented statistical methods, simulations based on artificial data are respectable. For higher dimensional multiple integral, Monte-Carlo numerical integration is, in general, better in quality than traditional numerical analysis techniques, since the error term is independent of the dimension. Monte-Carlo simulation provides us perspectives to unsolved problems and sometimes essential dicoveries also.

Monte-Carlo simulation as well as numerical integration need a huge amount of random numbers. Pseudorandom numbers according to a probability distribution may be transformed from pseudorandom numbers from the uniform distribution on the unit interval. To obtain uniform pseudorandom numbers, firstly we generate a sequence of integers mod m, next divide this sequence by m. It is, therefore, important to study distribution properties for integer sequences mod m.

An integer sequence $a = \{ a_n \}_{n=1,2,\ldots}$ is said to be uniformly distributed mod m, if, for any integer j with

$0 \leq j \leq m - 1$,

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

where $A_N(a ; j)$ is the number of a_n, $1 \leq n \leq N$ satisfying

$$a_n \equiv j \pmod m .$$

I. niven introduced this notion from a general point of view and S. Uchiyama gave its characterization.

Instead of all residue classes with respect to a given modulus m, we consider uniform distribution in residue classes (mod m) which are prime to m, that makes us possible mod m arithmetics.

We call an integer sequence $a = \{ a_n \}_{n=1,2,\dots}$ uniformly distributed in $(Z / mZ)^*$ if, for any integer relatively prime to m with $1 \leq j \leq m - 1$,

$$\lim_{N\to\infty} \frac{A_N(a ; j)}{N} = \frac{1}{\Phi (m)} ,$$

where $\Phi (\cdot)$ is the Euler function. This integer sequence is called also weakly uniformly distributed (mod m) according to W. Narkiewicz [2] .

The Dirichlet's prime number theorem gives us an example of uniformly distributed sequence in $(Z / mZ)^*$ for all positive integers $m \geq 2$. For other obtained results on weakly uniformly distributed sequences mod m, especially for multiplicative arithmetical functions, please consult the Narkiewicz's review [2], in which several unsolved problems on (weakly) uniformly distributed sequences of integers can also be found.

In this note we consider recursive sequences defined by

$$u_{n+1} \equiv u_n + u_n^{-1} \pmod m \qquad (1.1)$$

and shall prove in the next section that $\{ u_n \}_{n=1,2,\dots}$ is not

uniformly distributed in $(Z / mZ)^{*}$ except for $m = 3$. This proof given here is different from that in [1] . In the final section we shall give a generalization of the recursion formula (1.1) and obtain a similar result by using the idea in [1] .

2. RECURSIVE SEQUENCES DEFINED BY $u_{n+1} \equiv u_n + u_n^{-1} \pmod m$.

Recursive sequences defined by

$$h_{n+2} = h_{n+1} + h_n \qquad (2.1)$$

have a wide literature. This sequence with its initial value

$$h_1 = h_2 = 1$$

is the sequence of Fibonacci numbers, which is shown not to be uniformly distributed mod m except for $m = 5^k$, $k = 1,2,\cdots$, by H. Niederreiter [3] .

A variation of the recursion formula

$$h_{n+2} = a \cdot h_{n+1} + b \cdot h_n \qquad (2.2)$$

generates a sequence of generalized Fibonacci numbers and if this sequence is uniformly distributed mod m , then m is necessarily of the form $(a^2 - 4b)^k$, $k = 1,2,\cdots$.

Replacing (2.1) by

$$u_{n+1} \equiv u_n + u_n^{-1} \pmod m \qquad (2.3)$$

or by

$$u_{n+1} \equiv a \cdot u_n + b \cdot u_n^{-1} \pmod{m}, \qquad (2.4)$$

how the distribution of recursive sequences $\{ u_n \}_{n=1,2,\ldots}$ behaves mod m ? This problem was posed by M. Mendes France.

Before answering to this problem, it seems important to check that the recursive sequence $\{ u_n \}$ does not terminates. For this end, the following congruential equation

$$s + s^{-1} \equiv c \pmod{m} \qquad (2.5)$$

shold be soluble for all s in $(Z / mZ)^*$. The law of reciprocity affods us a satisfactory answer, (see [1] in detais).

Let us consider a necessary condition for the recursive sequence $\{ u_n \}$ to be uniformly distributed in $(Z / mZ)^*$.

LEMMA 1. If the recursive sequence $\{ u_n \}$ defined by (2.3) is uniformly distributed in $(Z / mZ)^*$, then it is necessary that

$$\begin{aligned} (u_1 + u_1^{-1})^k &\equiv u_2^k \pmod{m} \\ (u_2 + u_2^{-1})^k &\equiv u_3^k \pmod{m} \\ &\cdots\cdots \\ (u_{\phi(m)} + u_{\phi(m)}^{-1})^k &\equiv u_1^k \pmod{m}, \end{aligned} \qquad (2.6)$$

for every positive integer k .

For any even modulus m , the recrsion formula (2.3) ter-

minates immediately. For a prime p of the form $4\ell + 1$ and for its power p^n, no recursive sequence $\{ u_n \}$ is uniformly distributed in either $(Z / pZ)^*$ or $(Z / p^nZ)^*$. So our concern is restricted to primes of the form $4\ell + 3$.

LEMMA 2. For any prime p of the form $4\ell + 3$, no sequence $\{ u_n \}$ is uniformly distributed in $(Z / pZ)^*$ except for $m = 3$.

PROOF: Suppose that $\{ u_n \}$ is uniformly distributed in $(Z / pZ)^*$, and consider (2.6) for $p = 2$. Summing up these congruences with the remark

$$\{ u_1, u_2, \cdots, u_{\phi(m)} \} = (Z / mZ)^*, \qquad (2.7.)$$

we have

$$2(p - 1) + \sum_{i=1}^{p-1} i^2 \equiv 0 \ (\mathrm{mod}\ p) .$$

6 divides $(p-1)(2p - 1)$ for any prime number $p > 3$, then

$$2(p - 1) \equiv 0 \ (\mathrm{mod}\ p) ,$$

which is impossible for odd prime p. Thus we have one exception for $p = 3$.

COROLLARY. For any prime p of the form $4\ell + 3$, no sequence $\{ u_n \}$ is uniformly distributed in $(Z / p^nZ)^*$ except for $p = 3$.

LEMMA 3: For $n > 1$, no sequence $\{ u_n \}$ is uniformly

distributed in $(Z / 3^n Z)^*$.

PROOF: Suppose the contrary, then (2.6) for $k = 3$ with the consideration of (2.7) gives

$$3 \cdot \sum_{\substack{j=1 \\ (j,3^n)=1}}^{j=3^n-1} j + 3 \cdot \sum_{\substack{j=1 \\ (j,3^n)=1}}^{j=3^n-1} j^{-1} + \sum_{\substack{j=1 \\ (j=3^n)=1}}^{j=3^n-1} j^{-3} \equiv 0 \pmod{3^n} .$$

This congruence may be rewritten by

$$3 \cdot \sum_{\substack{j=1 \\ (j,3^n)=1}}^{j=3^n-1} j^4 + 3 \cdot \sum_{\substack{j=1 \\ (j,3^n)=1}}^{j=3^n-1} j^{-2} + \sum_{\substack{j=1 \\ (j=3^n)=1}}^{j=3^n-1} 1 \equiv 0 \pmod{3^n} .$$

The first and the second terms above are congruent to 0 (mod 3^n) but the third term

$$\phi(3^n) = 2 \cdot 3^{n-1}$$

is not congruent to 0 (mod 3^n) for $n > 1$.

From these lemmas, we obtain

THEOREM 1. No recursive sequence $\{ u_n \}$ defined by (2.3) is uniformly distributed in $(Z / mZ)^*$ except for $m = 3$.

2. SYMMETRIC FUNCTIONAL EQUATION.

In my paper [1] , Theorem 1 is a direct consequence of the next Theorem.

THEOREM 2. No recursive sequence $\{ u_n \}$ defined by (2.4)

is uniformly distributed in $(Z / mZ)^{*}$ except for $a = b = 1$ and $m = 3$.

Through our personal communications, Professor Doctor H. Niederreiter proposed an elegant proof of Theorem 2 (and also Theorem 1) in place of my long proof before. His idea is as follows:

Consider the corresponding function f to the recursion formula (2.4) . This function is defined by

$$f (s) = a \cdot s + b \cdot s^{-1}$$

on $(Z / mZ)^{*}$. If the recursive sequence $\{ u_n \}$ is uniformly distributed in $(Z / mZ)^{*}$, then f is bijective on $(Z / mZ)^{*}$. On the other hand, f satisfies

$$f (s) = f (b \cdot a^{-1} \cdot s^{-1})$$

for all $s \in (Z / mZ)^{*}$, which signifies

$$s \equiv b \cdot a^{-1} \cdot s^{-1} \pmod{m} , \qquad (3.1)$$

since f is a bijection on $(Z / mZ)^{*}$. Setting $s = 1$ and $s = 2$, we get the result.

Professor Niederreiter suggested me also the applicability of his idea to other classes of recursive sequences. One of the answer is the following:

Let us consider recursive sequences defined by

$$v_{n+1} \equiv a_k (v_n^k + v_n^{-k}) + a_{k-1} (v_n^{k-1} + v_n^{-(k-1)}) +$$

$$\cdots + a_1 (v_n + v_n^{-1}) + a_0 \pmod m . \qquad (3.2)$$

The corresponding function g from $(Z / mZ)^*$ is defined by

$$g (s) = a_k (s^k + s^{-k}) + a_{k-1} (s^{k-1} + s^{-(k-1)}) +$$

$$\cdots + a_1 (s + s^{-1}) + a_0 ,$$

which satisfies a functional equation

$$g (s) = g (s^{-1}) .$$

For odd m, $(Z / mZ)^*$ contains 2 as an element, then substituting 2 in

$$s \equiv s^{-1} \pmod m , \qquad (3.3)$$

we have $m = 3$. For even m, we denote the smallest element r in $(Z / mZ)^*$ other than the unit and setting r in (3.3) gives $m = r^2 - 1$. Then $r^2 - 1$ should be divided by all primes less than r, which holds for only small values of r from the prime number theorem.

Calculations in $(Z / 8Z)^*$ and $(Z / 24Z)^*$ finally shows the next Theorem:

THEOREM 3. No recursive sequence $\{ v_n \}$ defined by (3.2) is uniformly distributed in $(Z / mZ)^*$ except for $m = 3$ and

$$u_{n+1} \equiv u_n + u_n^{-1} \pmod 3 ,$$

$$v_{n+1} \equiv v_n^2 + v_n + 1 + v_n^{-1} + v_n^{-2} \pmod 3 .$$

REFERENCES

[1] NAGASAKA,K.: Distribution Property of Recursive Sequences Defined by $u_{n+1} \equiv u_n + u_n^{-1} \pmod m$, Fibonacci Q.,22,76-81 (1984).

[2] NARKIEWICZ,W.: Uniform Distribution of Sequences of Integers, Journées Arithmétiques 1980, Edited by J.V.Armitage, London Mathematical Society, Lecture Note Series 56, Cambridge University Press,202-210 (1982).

[3] NIEDERREITER,H.: Distribution of Fibonacci Numbers Mod 5^k, Fibonacci Q.,10,373-374 (1972).