◆◇◆◇◆

DISTRIBUTION PROPERTY OF RECURSIVE SEQUENCES DEFINED BY $u_{n+1} \equiv u_n + u_n^{-1}$ (MOD m)

KENJI NAGASAKA
Shinsyu University, 380 Nagano, Japan

(Submitted July 1982)

1. INTRODUCTION

We shall consider a distribution property of sequences of integers. Let us denote $a = (a_n)_{n \in \mathbf{N}}$ an infinite sequence of integers. For integers $N \geqslant 1$, $m \geqslant 2$, and j $(0 \leqslant j \leqslant m-1)$, let us define $A_N(j, m, a)$ as the number of terms among $a_1, a_2, \ldots, a_N$ satisfying the congruence $a_n \equiv j \pmod{m}$.

A sequence $a = (a_n)_{n \in \mathbf{N}}$ is said to be uniformly distributed modulo m (u.d. mod m) if, for every $j = 0, 1, \ldots, m-1$,

$$\lim_{N \to \infty} \frac{A_N(j, m, a)}{N} = \frac{1}{m}. \tag{1.1}$$

A sequence $a = (a_n)_{n \in \mathbf{N}}$ is said to be uniformly distributed in $\mathbf{Z}$ if, for any integer $m \geqslant 2$, $a = (a_n)_{n \in \mathbf{N}}$ is uniformly distributed modulo m.

This notion was first introduced by Niven [6] and various results are already obtained (see Kuipers & Niederreiter's book [4]), among which the sequence of Fibonacci numbers and its generalizations were investigated with respect to uniform distribution property modulo m. The sequence of generalized Fibonacci numbers is defined by the following linear recurrence formula of second order,

$$h_{n+2} = h_{n+1} + h_n \quad (n \geqslant 1), \tag{1.2}$$

with initial values $h_1 = a$ and $h_2 = b$.

The sequence of Fibonacci numbers $(h_n)_{n \in \mathbf{N}}$ with $h_1 = h_2 = 1$ is not uniformly distributed mod m for any $m \neq 5^k$ $(k = 1, 2, \ldots)$. Any sequence of generalized Fibonacci numbers is not uniformly distributed mod m for any $m \neq 5^k$ $(k = 1, 2, \ldots)$ and even for $m = 5^k$ $(k = 1, 2, \ldots)$ for certain initial values a and b [3].

Various modifications for the recurrence formula (1.2) can be considered. In this note we shall consider the following congruential recurrence formula:

$$u_{n+1} \equiv u_n + u_n^{-1} \pmod{m}. \tag{1.3}$$

Since our interest is the distribution property of integer sequences modulo m, the congruential recurrence will be sufficient for our purpose.

For two given integers s and m, where $m \geqslant 2$ is the modulus and $s = u_1$ is the starting point, we can generate a sequence of integers $u = u(s, m)$ mod m by the recurrence formula (1.3). We give our attention only to infinite sequences, and the set of these starting points is denoted by A_m.

The structure of A_m will be discussed in the next section. Similarly to the notion of uniform distribution modulo m, we define the function $A_N(j, m, u(s, m))$ for j each invertible element in the ring $\mathbf{Z}/m\mathbf{Z}$, and we call $u = u(s, m)$ for $s \in A$ uniformly distributed in $(\mathbf{Z}/m\mathbf{Z})^*$ if, for any invertible element $j \in \mathbf{Z}/m\mathbf{Z}$,

$$\lim_{N \to \infty} \frac{A_N(j, m, u(s, m))}{N} = \frac{1}{\phi(m)},$$

where $\phi(\cdot)$ denotes the Euler function.

It will be proved that recursive sequences $u(s, m)$ are not uniformly distributed in $(\mathbf{Z}/m\mathbf{Z})^*$ except for $m = 3$.

Finally, we generalize the recurrence formula (1.3) as

$$u_{n+1} \equiv au_n + bu_n^{-1} \pmod{m},$$

and a similar result will be given.

2. THE STRUCTURE OF A_m

We consider the solvability of the congruence

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

in $(\mathbf{Z}/m\mathbf{Z})^*$.

Case I: m is even

In this case, invertible elements in $\mathbf{Z}/m\mathbf{Z}$ are odd and their inverses are necessarily odd. Therefore, the sum of an invertible element and its inverse is even. Here we get

Theorem 1: If m is even, then $A_m = \phi$.

Case II: $m = p$ (odd prime)

In this case, the only noninvertible element in $\mathbf{Z}/p\mathbf{Z}$ is 0, so we can start with any starting point s, except 0, the recurrence

$$u_{n+1} \equiv u_n + u_n^{-1} \pmod{p}.$$

We consider the condition on $s \in (\mathbf{Z}/p\mathbf{Z})^*$ for which

$$s + s^{-1} \equiv 0 \pmod{p}. \tag{2.1}$$

This congruence is equivalent to

$$s^2 \equiv -1 \pmod{p}, \tag{2.2}$$

since s and p are relatively prime.

The first complementary law of reciprocity [1] shows that for any odd prime p,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \tag{2.3}$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol. Thus, we have

Theorem 2:

i) For any prime p of the form $4n + 3$,

$$A_p = (\mathbf{Z}/p\mathbf{Z})^*.$$

ii) For any prime p of the form $4n + 1$, no sequences $u(s, p)$ are uniformly distributed in $(\mathbf{Z}/p\mathbf{Z})^*$ for any starting point $s \in (\mathbf{Z}/p\mathbf{Z})^*$.

Case III: m is a power of an odd prime p

In this case, $m = p^\alpha$, $\alpha > 1$, and we shall consider the following congruence,

$$s + s^{-1} \equiv a \pmod{p^\alpha},$$

where $s \in (\mathbf{Z}/p^\alpha\mathbf{Z})^*$ and p divides a. This is equivalent to

$$s^2 \equiv as - 1 \pmod{p^\alpha}, \tag{2.4}$$

since s and p^α are relatively prime.

Letting $f(x) = x^2 - ax + 1$, then $f'(x) = 2x - a$. If the congruence

$$s^2 \equiv as - 1 \pmod{p} \tag{2.5}$$

has a solution s_0, then (2.4) has a solution, since

$$f'(s_0) = 2s_0 - a \equiv 2s_0 \not\equiv 0 \pmod{p}.$$

But (2.5) is identical to (2.2) because p divides a. Thus, we have

Theorem 3: Let $m = p^\alpha$ with $\alpha > 0$ and p an odd prime.

i) If p is of the form $4n + 3$, then $A_{p^\alpha} = (\mathbf{Z}/p^\alpha\mathbf{Z})^*$.

ii) If p is of the form $4n + 1$, then no $u(s, p^\alpha)$ is uniformly distributed in $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$.

Case IV: m is odd

In this case,

$$m = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

where the p_i's are odd primes and $\alpha_i > 0$.

Considering the congruence,

$$s^2 - as + 1 \equiv 0 \pmod{m},$$

where a divides m, the solvability of

$$s^2 - as + 1 \equiv 0 \pmod{p_i}$$

depends on the value $\left(\frac{a^2 - 4}{p_i}\right)$. Thus, we cannot conclude, as in previous cases, that the structure of A_m is in a compact form.

3. DISTRIBUTION PROPERTY OF $u(s, m)$

In the preceding section, we saw that for infinitely many m, $A_m \neq \phi$. We shall prove in this section that the distribution property of $u(s, m)$ is quite similar to that of the sequence of Fibonacci numbers.

Direct calculation gives

Theorem 4: For any $s \in A_3 = (\mathbf{Z}/3\mathbf{Z})^*$, $u(s, 3)$ is uniformly distributed in $(\mathbf{Z}/3\mathbf{Z})^*$.

We now present the main statement of the paper as Theorem 5.

Theorem 5: Let m be a positive integer greater than 1 satisfying $A_m \neq \phi$. For any $s \in A_m$, $u(s, m)$ is not uniformly distributed in $(\mathbf{Z}/m\mathbf{Z})^*$, except for $m = 3$.

We now generalize the recurrence formula (1.3) as follows:

$$u_{n+1} \equiv au_n + bu_n^{-1} \pmod{m}, \tag{3.2}$$

where a and b are invertible elements in $\mathbf{Z}/m\mathbf{Z}$. The sequence generated by (3.2) is denoted by $u(s; a, b, m)$, where $s = u_1$ is the invertible starting value, and the set of starting values that generates infinite sequences is written as $A_{m;a,b}$.

Similarly to Theorem 3, for even m, $A_{m;a,b} = \phi$. We do not mention the structure of $A_{m;a,b}$ since the distribution property of $u(s; a, b, m)$ is in question.

Theorem 6: For any s contained in nonempty $A_{m;a,b}$, no sequence $u(s; a, b, m)$ is uniformly distributed in $(\mathbf{Z}/m\mathbf{Z})^*$, except in the case of Theorem 4.

Proof: As Theorem 6 includes Theorem 5, we only give the proof of the latter.

We know that we only have to consider odd m greater than 2. If a sequence generated by (3.2) is uniformly distributed in $G = (\mathbf{Z}/m\mathbf{Z})^*$, then every element of G must appear in the sequence (considered mod m). In particular, for every $c \in G$, there exists $s \in G$ with

$$as + bs^{-1} \equiv c \pmod{m}.$$

Hence the function $f: G \to \mathbf{Z}/m\mathbf{Z}$, defined by

$$f(s) = as + bs^{-1},$$

is a bijection of G. But

$$f(s) = f(ba^{-1}s^{-1})$$

for all $s \in G$, and since f is a bijection, we get

$$s \equiv ba^{-1}s^{-1} \pmod{m};$$

hence,

$$s^2 \equiv ba^{-1} \pmod{m}$$

for all $s \in G$. Setting $s = 1$ gives

$$ba^{-1} \equiv 1 \pmod{m},$$

and setting $s = 2$ gives $m = 3$.

Inspection shows that only the case $a = b = 1$ yields a uniformly distributed sequence in $(\mathbf{Z}/3\mathbf{Z})^*$. Q.E.D.

ACKNOWLEDGMENT

I wish to express my sincere thanks to the referee for his comments, and expecially for his simple proofs of Theorems 5 and 6.

REFERENCES

1. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 5th ed. Oxford: Clarendon, 1979.
2. L. Kuipers & J.-S. Shiue. "On the Distribution Modulo m of Sequences of Generalized Fibonacci Numbers." *Tamkang J. Math.* 2 (1971):181-86.
3. L. Kuipers & J.-S. Shiue. "A Distribution Property of the Sequence of Fibonacci Numbers." *The Fibonacci Quarterly* 10 (1972):375-76, 392.
4. L. Kuipers & H. Niederreiter. *Uniform Distribution of Sequences.* New York-London-Sydney-Toronto: John Wiley & Sons, 1974.
5. H. Niederreiter. "Distribution of Fibonacci Numbers Mod 5^k." *The Fibonacci Quarterly* 10 (1972):373-74.
6. I. Niven. "Uniform Distribution of Sequences of Integers." *Trans. Amer. Math. Soc.* 98 (1961):52-61.

◆◇◆◇◆