Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Lawrence Kuipers, Jau-shyong Shiue

A distribution property of a linear recurrence of the second order

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **52** (1972), n.1, p. 6–10.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1972_8_52_1_6_0>

Teoria dei numeri. — *A distribution property of a linear recurrence of the second order.* Nota di LAWRENCE KUIPERS e JAU-SHYONG SHIUE, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Si ottengono proprietà di distribuzione uniforme relative a successioni di interi definite da certe formule ricorrenti rispetto ad un modulo che sia potenza di un numero primo.

Let A, B, a and b be fixed rational integers, let A and B be different from zero and let the equation $z^2 - Az - B = 0$ have distinct nonzero roots. Let a and b be not both equal to zero. Consider the linear recurrence of the second order (G_n), defined by

$$(1) \qquad G_0 = a \quad , \quad G_1 = b \quad , \quad G_{n+1} = AG_n - BG_{n-1} , \qquad n = 1, 2, \cdots .$$

In the present paper we establish a uniform distribution property of the above recurrence (G_n) with regard to a modulus m being equal to a power of a prime p under certain assumptions concerning the period $k(p^h)$ of (G_n) modulo m.

Definition of uniform distribution mod m. Let m be an integer ≥ 2 and let (x_n), $n = 1, 2, \cdots$ be a sequence of integers. Let j be any element of the set $\{0, 1, \cdots, m-1\}$. Let N be an arbitrary positive integer. Let $A(N, j, m)$ denote the number of (x_n), $n = 1, 2, \cdots, N$, that are congruent to j mod m. The sequence (x_n) is said to be uniformly distributed mod m if

$$(2) \qquad \lim_{N\to\infty} A(N, j, m)/N = 1/m \qquad \text{for} \quad j = 0, 1, \cdots, m-1 \quad [1].$$

Let p be a prime number and let $m = p^h$ $(h = 1, 2, \cdots)$. Let $k = k(p^h)$ the least positive integer for which both congruences

$$G_k \equiv G_0 \pmod{p^h} \quad , \quad G_{k+1} \equiv G_1 \pmod{p^h}$$

are satisfied. The integer $k(p^h)$ is the least period of (G_n). That such periods exist and can be evaluated, if a, b, A and B are given, follows from the fundamental theorem on purely periodic sequences due to Morgan Ward [2].

We want to establish the following result.

THEOREM. *Let p be a prime and let* (1) *be a linear recurrence of the second order such that*

$$p > 2 \quad , \quad p \mid (A^2 - 4B) \quad , \quad (A, p) = 1 \quad , \quad (bA - 2aB, p) = 1$$

(*) Nella seduta del 15 gennaio 1972.

It is assumed that $k(p^h) = (p - 1)\,p^h$ *is the smallest period of* (G_n) mod p^h, $h = 1, 2, \cdots$. *Furthermore it is assumed that the congruence* $2Bx \equiv A \pmod{p}$ *is satisfied by a primitive root* mod p. *Then the sequence* (G_n) *is uniformly distributed* mod p^h *for* $h = 1, 2, \cdots$

Proof. We prove the theorem first for $h = 1$. Upon reduction mod p the terms of the reduced sequence (G_n) assume only values taken from the set $\{0, 1, \cdots, p-1\}$. There are $p^2 - 1$ distinct pairs of two consecutive terms, since the occurrence of the pair $0, 0$ would imply $a = 0$, $b = 0$. The period in the case $h = 1$ according to the assumption is equal to $(p-1)\,p$, so the period shows already $p^2 - p$ distinct pairs of two consecutive terms. There is however a string of $p - 1$ elements, namely the residues mod p of the integers

$$(3) \qquad g^{p-1}, g^{p-2}, \cdots, g^2, g, 1,$$

where g is a primitive root mod p satisfying $2Bx \equiv A \pmod{p}$, no two consecutive elements of which occur in the above period of $(p-1)\,p$ elements. This can be seen as follows. We have according to the assumption $p \mid (A^2 - 4B)$ and $p > 2$. So the relation $(2Bg - A)^2 \equiv A^2 - 4B \pmod{p}$ can be written in the form

$$Bg^2 - Ag + 1 \equiv 0 \pmod{p},$$

which implies

$$Bg^3 - Ag^2 + g \equiv 0 \pmod{p},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$Bg^{p-1} - Ag^{p-2} + g^{p-3} \equiv 0 \pmod{p},$$

from which can be seen that the pair $g^{p-1}, g^{p-2} \pmod{p}$ according to (1) is followed by $g^{p-2}, g^{p-3} \pmod{p}$, etcetera. None of these pairs occurs in the above period of length $(p-1)\,p$.

The maximal number of times that each of the residues $0, 1, \cdots, p-1$ appears the collection of all distinct pairs is $2p$. Each of the residues $1, 2, \cdots, p-1$ occurs twice in the set of pairs of consecutive residues taken from (3). Hence the maximal number of each of the residues $1, 2, \cdots, p-1$ occurring in the period of length $(p-1)\,p$ is reduced to $2p - 2$. Moreover the two residues 0 from the pair $0, 0$ have to be discarded. So the number of all residues occurring in that period does not exceed $p(2p-2) = 2p(p-1)$. Since the number of pairs of consecutive elements is equal to $p(p-1)$, we see that the residues $0, 1, \cdots, p-1$ are equally distributed over this period, in fact each residue occurs $p-1$ times. Because of the periodical continuation the recurrence is uniformly distributed mod p. Hence the theorem is true for $h = 1$.

Now assume the theorem is true in the case $h - 1$, or it is supposed that the least period of (G_n) modulus p^{h-1} of length $k(p^{h-1}) = (p-1)\,p^{h-1}$ shows exactly $p - 1$ times each residue mod p^{h-1}.

Let e be any integer with $0 \leq e \leq p^h - 1$. Then the congruence

$$(4) \qquad G_n \equiv e \pmod{p^{h-1}}$$

is satisfied by exactly $p - 1$ indices n between 0 and $(p-1)p^{h-1} - 1$. Let C be the set of these indices. Now suppose that the congruence

$$(5) \qquad G_n \equiv e \pmod{p^h}, \qquad 0 \leq n \leq (p-1)p^h - 1$$

is satisfied by some n, then by periodicity

$$n \equiv c \pmod{(p-1)p^{h-1}} \qquad \text{for some} \quad c \in C.$$

In the other direction we want to show that to any index $c \pmod{(p-1)p^{h-1}}$ with $G_c \equiv e \pmod{p^{h-1}}$ there corresponds at most one index $n \pmod{(p-1)p^h}$ satisfying

$$(6) \qquad G_n \equiv e \pmod{p^h} \quad , \quad c \equiv n \pmod{(p-1)p^{h-1}}.$$

In order to do that let us suppose that we have besides (6) also

$$G_m \equiv e \pmod{p^h}, \qquad 0 \leq m \leq (p-1)p^h - 1,$$
$$m \equiv c \pmod{(p-1)p^{h-1}} \quad , \quad n \geq m.$$

Then in particular

$$(7) \qquad G_n \equiv G_m \pmod{p^h} \qquad \text{and} \quad n \equiv m \pmod{(p-1)p^{h-1}}.$$

In order to investigate the system (7) we use suitable representations for G_n.

Let θ_1 and θ_2 be the distinct roots of the quadratic equation $x^2 - Ax + B = 0$. Then

$$(8) \qquad \theta_1 = \frac{1}{2}(A + \sqrt{A^2 - 4B}) \qquad \text{and} \quad \theta_2 = \frac{1}{2}(A - \sqrt{A^2 - 4B}),$$

and G_n can be written in the form

$$(9) \qquad G_n = \frac{(b - a\theta_2)\,\theta_1^n - (b - a\theta_1)\,\theta_2^n}{\theta_1 - \theta_2}, \qquad n = 0, 1, 2, \cdots.$$

By substituting (3) in (4) we obtain for G_n the following expression

$$(10) \qquad G_n = \frac{1}{2^{n-1}} \left\{ b \sum_{j=0}^{\infty} \binom{n}{2j+1} (A^2 - 4B)^j A^{n-2j-1} - \right.$$
$$\left. - 2aB \sum_{j=0}^{\infty} \binom{n-1}{2j+1} (A^2 - 4B)^j A^{n-2j-2} \right\}, \qquad n = 1, 2, \cdots,$$

in which $\binom{n}{k}$ stands for zero if $k > n$.

Now the first congruence of (7) becomes

$$\frac{1}{2^{n-1}} \left\{ b \sum_{j=0}^{\infty} \binom{n}{2j+1} (A^2 - 4B)^j A^{n-2j-1} - 2aB \sum_{j=0}^{\infty} \binom{n-1}{2j+1} (A^2 - 4B)^j A^{n-2j-2} \right\}$$

$\equiv$ same expression with m instead of $n \pmod{p^k}$, or after multiplication of both members by 2^{n-1},

$$b \sum_{j=0}^{\infty} \binom{n}{2j+1} (A^2 - 4B)^j A^{n-2j-1} - 2aB \sum_{j=0}^{\infty} \binom{n-1}{2j+1} (A^2 - 4B)^j A^{n-2j-2} \equiv$$

$$\equiv 2^{n-m} \left\{ b \sum_{j=0}^{\infty} (A^2 - 4B)^j \binom{m}{2j+1} A^{m-2j-1} - \right.$$

$$\left. - 2aB \sum_{j=0}^{\infty} \binom{m-1}{2j+1} (A^2 - 4B)^j A^{m-2j-2} \right\} \pmod{p^h}.$$

We have $2(p-1)p^{h-1} \equiv 1 \pmod{p^h}$, and because of the second congruence of (6) we obtain

$$2^{n-m} \equiv 1 \pmod{p^h}.$$

Hence, taking also into account that $p \mid (A^2 - 4B)$, we write the congruence under investigation in the following form:

$$(11) \qquad b \sum_{j=0}^{h-1} (A^2 - 4B)^j \left\{ \binom{n}{2j+1} A^{n-2j-1} - \binom{m}{2j+1} A^{m-2j-1} \right\} -$$

$$- 2aB \sum_{j=0}^{h-1} (A^2 - 4B)^j \left\{ \binom{n-1}{2j+1} A^{n-2j-1} - \binom{m-1}{2j+1} A^{m-2j-2} \right\} \equiv 0 \pmod{p^h}.$$

Now

$$\binom{n}{2j+1} A^{n-2j-1} - \binom{m}{2j+1} A^{m-2j-1} = A^{m-2j-1} \left\{ \binom{n}{2j+1} A^{n-m} - \binom{m}{2j+1} \right\},$$

and since $(p-1)p^{h-1} \mid (n-m)$ and $(A, p) = 1$, the last expression is congruent to

$$A^{m-2j-1} \left\{ \binom{n}{2j+1} - \binom{m}{2j+1} \right\} \pmod{p^h},$$

since $A^{n-m} \equiv 1 \pmod{p^h}$. Hence (11) can be written in the form

$$(12) \qquad b \sum_{j=0}^{h-1} (A^2 - 4B)^j A^{m-2j-1} \left\{ \binom{n}{2j+1} - \binom{m}{2j+1} \right\} -$$

$$- 2aB \sum_{j=0}^{h-1} (A^2 - 4B)^j A^{m-2j-2} \left\{ \binom{n-1}{2j+1} - \binom{m-1}{2j+1} \right\} \equiv 0 \pmod{p^h}.$$

Now consider the terms occurring on the left hand side of (12) with $j \geq 1$. The largest exponent l such that p divides $(2j+1)!$ satisfies

$$l = \sum_{i=1}^{\infty} \left[\frac{2j+1}{p^i} \right] < \sum_{i=1}^{\infty} \frac{2j+1}{p^i} < j, \qquad \text{since} \quad p > 2.$$

Hence the integers of the type $(A^2 - 4B)^j \binom{n}{2j+1}$ occuring as factors of terms in the above congruence (12) contain at least one factor p. Moreover the expressions

$$(2j+1)!\left\{\binom{n}{2j+1}-\binom{m}{2j+1}\right\} \quad \text{and} \quad (2j+1)!\left\{\binom{n-1}{2j+1}-\binom{m-1}{2j+1}\right\}$$

contain the factor $n-m$ and hence the factor $(p-1)\,p^{h-1}$. Hence the terms in (12) with $j \geq 1$ all have p^h as divisor, and so (12) reduces to the term with $j=0$, or

$$bA^{m-1}(n-m) - 2\,aBA^{m-2}(n-m) \equiv 0 \pmod{p^h}$$

or

$$(n-m)(bA-2\,aB) \equiv 0 \pmod{p^h}.$$

This implies that $n \equiv m \pmod{p^h}$, since it is assumed that $(bA-2\,aB\,,p)=1$ and $(A\,,p)=1$. Hence $n=m$, and so we conclude that there are exactly $p-1$ elements of each residue class in the first period of $(p-1)\,p^h$ elements. This implies that because of periodicity the recurrence (G_n) is uniformly distributed mod p^h. Herewith the theorem is completely established.

Examples 1. By taking $a=1$, $b=1$, $A=1$, $B=-1$ one obtains the Fibonacci sequence which has mod 5^h the period $4\cdot 5^h$. Hence the Fibonacci sequence is uniformly distributed mod 5^h $(h=1\,,2\,,\cdots)$, a property already known [3].

2. The sequence obtained by taking $a=1\,,b=1\,,A=1\,,B=-3$, has mod 13^h the period $12\cdot 13^h$. The congruence $2\,Bx \equiv A \pmod{13}$ is satisfied by the primitive roots 2 (mod 13). Hence the sequence is uniformly distributed mod 13^h $(h=1\,,2\,,\cdots)$.

Unsolved problems. Take $a=1\,,b=1\,,A=3\,,B=-1$. The sequence has period $4.13^h \pmod{13^h}$. Is the sequence uniformly distributed mod 13^h? It is easily checked that this is the case for $h=1$. The same question arises in the cases $a=1\,,b=3\,,A=3\,,B=-1$ and $a=1\,,b=5\,,A=3$, $B=-1$.

References

[1] I. NIVEN, *Uniform distribution of sequences of integers*, «Trans. Amer. Math. Soc.», *98*, 52–61 (1961).

[2] M. WARD, *The arithmetical theory of linear recurring series*, «Trans. Amer. Math. Soc.», *35*, 600–628 (1933).

[3] H. NIEDERREITER, *Distribution of Fibonacci numbers mod 5^h*, Fibonacci Quarterly.