PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 48, Number 2, April 1975

LINEAR RECURRENCES AND UNIFORM DISTRIBUTION

MELVYN B. NATHANSON

ABSTRACT. A necessary and sufficient condition is obtained for the uniform distribution modulo p of a sequence of integers satisfying a linear recurrence relation.

Let $A = \{a_n\}_{n=1}^{\infty}$ be an infinite sequence of integers. For integers $m \geq 2$ and r, let $A(N, r, m)$ denote the number of terms a_n such that $n \leq N$ and $a_n \equiv r \pmod{m}$. If

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

for $r = 0, 1, \cdots, m-1$, then the sequence A is *uniformly distributed modulo* m. The sequence A is *uniformly distributed* if A is uniformly distributed modulo m for all $m \geq 2$.

Kuipers, Niederreiter, and Shiue [1], [2], [4] have proved that the Fibonacci numbers are uniformly distributed modulo m only for $m = 5^k$, and that the Lucas numbers are not uniformly distributed modulo m for any $m \geq 2$. Both the Lucas and Fibonacci numbers satisfy the linear recurrence $x_{n+2} = x_{n+1} + x_n$. In this note we consider the uniform distribution of an arbitrary linearly recurrent sequence of integers.

Theorem 1. *Let* $X = \{x_n\}_{n=1}^{\infty}$ *be a sequence of integers satisfying the linear recurrence* $x_{n+2} = ax_{n+1} + bx_n$. *Let* p *be an odd prime. Then the sequence* X *is uniformly distributed modulo* p *if and only if* $p \mid (a^2 + 4b)$, $p \nmid a$, *and* $p \nmid (2x_2 - ax_1)$. *The sequence* X *is uniformly distributed modulo* 2 *if and only if* $2 \mid a$, $2 \nmid b$, *and* $2 \nmid (x_2 - x_1)$.

Proof. The linearly recurrent sequence X is periodic modulo p. If the period of X is not divisible by p, then X is certainly not uniformly distributed modulo p. Zierler [5] showed that if $p \nmid (a^2 + 4b)$, then the period of X is relatively prime to p. If $p \mid (a^2 + 4b)$ and $p \mid a$, then $p \mid b$, and so $x_n \equiv 0 \pmod{p}$ for all $n \geq 3$. If $p \mid (a^2 + 4b)$ and $p \nmid a$, then

Presented to the Society, January 16, 1974 under the title *Uniform distribution and linear recurrences*; received by the editors February 4, 1974.

AMS (MOS) subject classifications (1970). Primary 10A35, 10F99.

Key words and phrases. Uniform distribution, recurrence sequences, linear recurrences, Hasse principle.

$$(*) \qquad x_n \equiv \frac{2}{a^2}(2x_2 - ax_1)n\left(\frac{a}{2}\right)^n - \frac{4}{a^2}(x_2 - ax_1)\left(\frac{a}{2}\right)^n \pmod{p}.$$

If $p|(2x_2 - ax_1)$, then $x_n \equiv t(a/2)^n \pmod{p}$ for some constant t. Either $t \equiv 0 \pmod{p}$, or the period of X is the exponent e of $a/2$ modulo p. But e is not divisible by p. Therefore, if X is uniformly distributed modulo p, then $p|(a^2 + 4b)$, $p \nmid a$, and $p \nmid (2x_2 - ax_1)$.

Conversely, suppose that X satisfies these three conditions. Let $A \equiv a/2 \pmod{p}$, and let e be the exponent of A modulo p. By $(*)$, there are constants s and t such that $p \nmid s$ and $x_n \equiv (sn + t)A^n \pmod{p}$ for all $n \geq 1$. This sequence has period ep modulo p. To show that X is uniformly distributed modulo p, it suffices to show that each distinct residue modulo p occurs exactly e times among the first ep terms of the sequence X.

Imagine these ep terms written in a matrix with e rows and p columns. For $i = 0, 1, \cdots, e-1$ and $j = 1, 2, \cdots, p$, let the (i, j)th component of this matrix be x_{ip+j}. The jth column of the matrix consists of the e elements x_{ip+j} with $i = 0, 1, \cdots, e-1$. But

$$x_{ip+j} \equiv (s(ip + j) + t)A^{ip+j} \equiv (sj + t)A^{j-i} \pmod{p}.$$

The set $\{A^{j-i}\}_{i=0}^{e-1}$ contains precisely the e residues $\{A^i\}_{i=0}^{e-1}$, and so the jth column of the matrix can be rearranged so that its (i, j)th entry is now $(sj + t)A^i$. Consider the ith row. It now consists of the p residues $(sj + t)A^i$ for $j = 1, 2, \cdots, p$. Since $s \not\equiv 0 \pmod{p}$, these residues are distinct modulo p, and so each row of the rearranged matrix contains a complete system of residues modulo p. That is, each residue modulo p occurs exactly e times in the first ep elements of the sequence X.

This proves the theorem for odd primes. The case $p = 2$ is trivial.

Theorem 2 (Hasse principle). *Let $X = \{x_n\}_{n=1}^{\infty}$ satisfy the linear recurrence $x_{n+2} = ax_{n+1} + bx_n$. Then X is uniformly distributed if and only if X is uniformly distributed modulo p for all primes p.*

Proof. If X is uniformly distributed modulo p for all primes p, then $p|(a^2 + 4b)$ for all p, and so $a^2 + 4b = 0$. Since a and b are relatively prime, it follows that $b = -1$ and $a = \pm 2$. If $a = 2$, then X is the arithmetic progression $x_n = (n-1)(x_2 - x_1) + x_1$, where $x_2 - x_1 = \pm 1$. If $n = -2$, then X is the sequence $x_n = (-1)^n[(n-1)(x_2 + x_1) - x_1]$, where $x_2 + x_1 = \pm 1$. In both cases, X is uniformly distributed.

The converse is trivial.

Remark. The sequence X is *p-adically uniformly distributed* if X is uniformly distributed modulo p^k for all $k \geq 1$. We can prove, by the method of [3], [4], the following "Hensel's lemma": If the linearly recurrent sequence X is uniformly distributed modulo p^2, then X is p-adically uniformly distributed.

R. T. Bumby has obtained similar results.

REFERENCES

1. L. Kuipers and J. S. Shiue, *A distribution property of the sequence of Lucas numbers*, Elem. Math. 27 (1972), 10–11. MR 46 #144.

2. ———, *A distribution property of the sequence of Fibonacci numbers*, Fibonacci Quart. 10 (1972), no. 4, 375–376, 392. MR 47 #3302.

3. ———, *A distribution property of a linear recurrence of the second order*, Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. 52 (1972), 6–10.

4. H. Niederreiter, *Distribution of Fibonacci numbers* mod 5^k, Fibonacci Quart. 10 (1972), no. 4, 373–374. MR 47 #3303.

5. N. Zierler, *Linear recurring sequences*, J. Soc. Indust. Appl. Math. 7 (1959), 31–48. MR 21 #781.

DEPARTMENT OF MATHEMATICS, SOUTHERN ILLINOIS UNIVERSITY, CARBONDALE, ILLINOIS 62901

Current address: School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540