PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 50, July 1975

A DISTRIBUTION PROPERTY FOR LINEAR RECURRENCE OF THE SECOND ORDER[1]

R. T. BUMBY

ABSTRACT. The collection of all numbers modulo which a given recurrent sequence can be uniformly distributed is determined.

Introduction. Given integers A, B, G_0, G_1, there is a unique sequence of integers $\langle G_n : n \geq 0 \rangle$ determined by $G_{n+1} = AG_n - BG_{n-1}$. If $A^2 \neq 4B$, then $G_n = \lambda\alpha^n + \lambda'\alpha'^n$ where α, α' are the roots of $x^2 - Ax + B = 0$ and λ, λ' are found by solving $\lambda + \lambda' = G_0$, $\lambda\alpha + \lambda'\alpha' = G_1$. From our assumptions it follows that α, α', $\lambda(\alpha - \alpha')$, $\lambda'(\alpha - \alpha')$ are all algebraic integers. In the case in which α is irrational, all lie in a quadratic extension and $'$ denotes conjugation in this field. The *degenerate case*, $A^2 = 4B$, is dealt with by writing $A = 2a$, $B = a^2$. Then $G_n = bna^{n-1} + ca^n$ with integers a, b, c. The degenerate case is similar to the local behavior at primes dividing $A^2 - 4B$ in the general case.

Reduction of $\langle G_n \rangle$ modulo m yields a periodic sequence (after perhaps some atypical initial terms). We may then define the distribution of G_n modulo m as the relative frequency of each residue in a full period. The sequence is said to be *uniformly distributed modulo* m if each residue occurs equally often. We wish to determine all moduli for which a given recurrent sequence is uniformly distributed. This will complete the study initiated by Kuipers and Shiue [1], [2]. Along the way we will relate the uniform distribution of $\langle G_n \rangle$ to that of $\langle G_{nk+i} \rangle$ for fixed i and k.

If $m_1 | m_2$ and a sequence is uniformly distributed modulo m_2, then it is clearly uniformly distributed modulo m_1. In the other direction, suppose p is a prime, $p \nmid m$, and the recurrent sequence $\langle G_n \rangle$ is uniformly distributed modulo mp^h for some $h \geq 0$. We find k such that $G_{n+k} \equiv G_n \pmod{mp^h}$ and consider all subsequences $\langle G_{nk+i} \rangle$. The $\langle G_{nk+i} \rangle$ are constant modulo mp^h. If each is uniformly distributed through the allowed values modulo

Received by the editors February 4, 1974.
AMS (MOS) subject classifications (1970). Primary 10A35.

[1]Work done at the NSF Summer Institute on Number Theory (Ann Arbor, Michigan, 1973).

p^{b+1}, then, by the Chinese remainder theorem, $\langle G_n \rangle$ is uniformly distributed modulo mp^{b+1}. Finally, if $\langle G_n \rangle$ is to be uniformly distributed modulo m, the period of $\langle G_n \rangle$ modulo m is necessarily divisible by m. These three observations form the basis of our method. When the study is limited to the powers of a single prime, we are dealing with a local problem. This allows us to multiply by any p-adic unit.

The degenerate case; prime modules. Using the formula $G_n = bna^{n-1} + ca^n$, we note that $p|a$ requires that $G_n \equiv 0 \pmod p$ for $n > 1$. Since this is far from uniformly distributed we discard those primes immediately and assume that a is a unit modulo p. Now

$$G_{n+k} - G_n = G_n(a^k - 1) + bka^{n+k-1}. \tag{1}$$

Apply (1) with k equal to the order of a mod p to get

$$G_{n+k} - G_n \equiv bka^{n+k-1} \pmod p. \tag{2}$$

Since $k|p-1$, it is relatively prime to p.

Proposition 1. *If $A = 2a$, $B = a^2$, then G_n is uniformly distributed modulo a prime p iff $p \nmid a(G_1 - aG_0)$. In fact, if $p \nmid a(G_1 - aG_0)$ there is a $k < p$ such that each subsequence $\langle G_{kn+i} \rangle$ is congruent to an arithmetic progression with nonzero difference modulo p. This property of the $\langle G_{kn+i} \rangle$ is preserved if k is replaced by any multiple which is also relatively prime to p.*

Proof. Our quantity $b = G_1 - aG_0$. If $p|ab$ then the period of $\langle G_n \rangle$ modulo p is relatively prime to p. On the other hand, if $p \nmid ab$, the second claim follows directly from (2). The third claim is immediate.

The nondegenerate case; prime modules. As in the degenerate case, if $p|(A, B)$ the sequence $\langle G_n \rangle$ becomes 0 mod p for $n > 1$. Discarding this case, we may assume that $(p, \alpha) = 1$. Then we have

$$G_{n+k} - G_n = G_n(\alpha^k - 1) + [\lambda'(\alpha' - \alpha)]\alpha'^n[(\alpha'^k - \alpha^k)/(\alpha' - \alpha)] \tag{3}$$

where both terms in brackets are algebraic integers. If $\mathfrak{p}$ denotes a prime over p in $\mathbf{Q}(\alpha)$ and k is the order of α mod $\mathfrak{p}$, then

$$G_{n+k} - G_n \equiv [\lambda'(\alpha' - \alpha)]\alpha'^n[(\alpha'^k - \alpha^k)/(\alpha' - \alpha)] \pmod{\mathfrak{p}}. \tag{4}$$

Since the G_n are rational integers, $G_{n+k} \equiv G_n \pmod{\mathfrak{p}}$ is equivalent to $G_{n+k} \equiv G_n \pmod p$. Here $(k, p) = 1$ since $k|p^2 - 1$ so if $G_{n+k} \equiv G_n \pmod{\mathfrak{p}}$, the sequence $\langle G_n \rangle$ is not uniformly distributed mod p. Thus $[\lambda'(\alpha' - \alpha)]$

$\in \mathfrak{p}$ or $\alpha' \in \mathfrak{p}$ will make uniform distribution impossible. We may then consider α' to be also a unit modulo p and adjust k, still dividing $p^2 - 1$, so that $\alpha^k \equiv \alpha'^k \equiv 1 \pmod{\mathfrak{p}}$. Since $\alpha^k - \alpha'^k \in \mathfrak{p}$, we must have $\alpha' - \alpha \in \mathfrak{p}$ if the third factor on the right side of (4) is not to be 0 mod $\mathfrak{p}$.

Proposition 2. *Suppose $A^2 \neq 4B$, and α, α' are the roots of $x^2 - Ax + B = 0$. Then $\langle G_n \rangle$ can be uniformly distributed* mod p *only for the finitely many primes for which $(\alpha - \alpha', p) \neq 1$. In this case, $\langle G_n \rangle$ is uniformly distributed* mod p *iff $(p, \alpha) = 1$ and $(p, G_1 - G_0\alpha) = 1$. Moreover, if these conditions are satisfied, there is $k | p^2 - 1$ such that each subsequence $\langle G_{nk+i} \rangle$ is congruent to an arithmetic progression with nonzero difference modulo p. The property of the $\langle G_{nk+i} \rangle$ is preserved if k is replaced by any multiple relatively prime to p.*

Proof. $G_1 - G_0\alpha = \lambda'(\alpha' - \alpha)$. If $\alpha' \equiv \alpha \pmod{\mathfrak{p}}$, then

$$(\alpha'^k - \alpha^k)/(\alpha' - \alpha) \equiv k\alpha^{k-1} \pmod{\mathfrak{p}}.$$

Thus (4) is completely analogous to (2) and Proposition 2 follows from it in the same way as Proposition 1 follows from (2).

Remark. $(\alpha - \alpha')^2 = A^2 - 4B$, so we are concerned with the primes dividing $A^2 - 4B$. $2\alpha \equiv A \pmod{\mathfrak{p}}$; so if $p \neq 2$, $\langle G_n \rangle$ is uniformly distributed modulo $p | A^2 - 4B$ iff $p \nmid A(2G_1 - AG_0)$. $\langle G_n \rangle$ is uniformly distributed mod 2 iff $2 | A$, $2 \nmid B(G_0 + G_1)$.

Example 1. Let $A = 1$, $B = -1$, so $A^2 - 4B = 5$. The only possible prime modulus of uniform distribution is 5. The condition for there to be no modulus of uniform distribution > 1 is that $5 | 2G_1 - G_0$. The Lucas numbers ($G_0 = 2$, $G_1 = 1$) have this property, hence have no modulus of uniform distribution (cf. [2]). The Fibonacci numbers ($G_0 = G_1 = 1$) do not; hence they are uniformly distributed modulo 5 (cf. [1]).

Example 2. Whenever $G_0 = 2$, $G_1 = A$, the criterion given in the remark above shows that there is no modulus of uniform distribution.

General moduli. We suppose that we have a modulus m all of whose prime divisors are moduli of uniform distribution. These are the only moduli we need test. Furthermore, by induction, it suffices to consider the case in which $m = m_0 q^{b+1}$, $\langle G_n \rangle$ is uniformly distributed modulo $m_0 q^b$, and all prime factors of m_0 are less than q. We discuss only the nondegenerate case, leaving the details of the degenerate case to the reader.

Suppose first that $b = 0$. The method described in the introduction depends on finding k such that $G_{n+k} \equiv G_n \pmod{m_0}$. Using (3) and the condition that α be a unit mod $\mathfrak{p}$, it is easy to find such a k composed of

primes $p|m_0$ and primes dividing p^2-1 for these values of p. The primes dividing p^2-1 are less than p except when $p=2$. However, if $\langle G_n \rangle$ is uniformly distributed mod 2, $G_{n+1} \equiv G_n + 1 \pmod 2$ and $\alpha \equiv 1 \pmod{\mathfrak{p}}$, so no difficulty arises in that case. In all cases, one has a quantity $k = k_0(q)$ such that $(q, k) = 1$, $G_{n+k} \equiv G_n \pmod{m_0}$ and $\alpha^k \equiv 1 \pmod{\mathfrak{q}}$. From the last part of Proposition 2, we conclude that *each* $\langle G_{kn+i} \rangle$ behaves like a *nontrivial* arithmetic progression mod $\mathfrak{q}$. Thus $h=0$ gives no difficulty.

Lemma. *If π is a prime element for a valuation extending the p-adic valuation on* $\mathbf{Q}$, *and if $c>0$ is maximal with $\beta \equiv 1 \pmod{\pi^c}$, then $\beta^p \equiv 1 \pmod{p\pi^c}$ but not $\pmod{p\pi^{c+1}}$ provided that $p\pi^{c+1}|\pi^{cp}$.*

Proof. Write $\beta = 1 + x\pi^c$ with x a unit modulo π and expand β^p by the binomial theorem. Since $p|\binom{p}{i}$ for $0<i<p$, we have $\beta^p \equiv 1 + px\pi^c + x^p\pi^{pc} \pmod{p\pi^{c+1}}$. The lemma is a special case of this formula.

In our case $p|(\pi)^2$ so that $p\pi^{c+1}|\pi^{cp}$ unless: (a) $\mathfrak{p}=(2)$, $c=1$; (b) $\mathfrak{p}^2=(2)$, $c \le 2$; (c) $\mathfrak{p}^2=(3)$, $c=1$.

Furthermore, only in case (b) with $c=1$ do we fail to have $\beta^p \equiv 1 \pmod{p\pi^c}$.

We pause to examine the exceptional case in which $\mathfrak{q}^2=(2)$, $\alpha \equiv 1 \pmod{\mathfrak{q}}$, $\alpha \not\equiv 1 \pmod 2$. Writing $\alpha = 1+\pi$, $\alpha' = 1+\pi'$, we have

$$\begin{aligned} G_{n+2} - G_n &= G_n(\alpha^2-1) + [G_1 - G_0\alpha]\alpha'^n(\alpha'+\alpha) \\ &\equiv \pi^2 G_n + (2+\pi+\pi') \pmod{2\mathfrak{q}}. \end{aligned}$$

If $\pi+\pi' \equiv 2 \pmod 4$, then $G_{n+2} \equiv -G_n \pmod 4$; so either 0 or 2 is omitted. If $\pi+\pi' \equiv 0 \pmod 4$, then $G_{n+2} \equiv 2 - G_n \pmod 4$; so either 1 or -1 is omitted. Thus $\langle G_n \rangle$ is not uniformly distributed modulo 4, or any multiple of 4. Consequently, if $\langle G_n \rangle$ is uniformly distributed modulo 4, $\alpha \equiv 1 \pmod 2$. This is equivalent to $A - B \equiv 1 \pmod 4$.

Now, if $q=2$, we will assume $\alpha \equiv 1 \pmod 2$. For other q, no restriction is required. We have already constructed $k_0(q)$ and now we define $k_h(q)$ inductively by $k_{h+1}(q) = q \cdot k_h(q)$. We certainly have $\alpha^k \equiv 1 \pmod{q^h\mathfrak{q}}$ for $k = k_h(q)$. Thus we get

$$(5) \qquad G_{n+k} - G_n \equiv [\lambda'(\alpha'-\alpha)]\alpha'^n[(\alpha'^k - \alpha^k)/(\alpha'-\alpha)] \pmod{q^h\mathfrak{q}}$$

with $k = k_h(q)$. By Proposition 2, the result we seek is equivalent to $(\alpha'^k - \alpha^k)/(\alpha'-\alpha) \not\equiv 0 \pmod{q^h\mathfrak{q}}$; and this has been established for $h=0$. Since α is a unit modulo $\mathfrak{q}$, there is no difficulty in working with α as a $\mathfrak{q}$-adic unit. Thus we must show that $\beta = \alpha'/\alpha$ satisfies $(\beta^k - 1)/(\beta - 1)$

$\not\equiv 0 \pmod{q^h \mathfrak{q}}$. Since q has been chosen to satisfy Proposition 2, this holds for $h = 0$. Unless $(\beta^k - 1) \mid (2)$ or (3), the Lemma gives $(\beta^{kq} - 1)/(\beta^k - 1) \equiv q \pmod{q\,\mathfrak{q}}$. This gives the desired conclusion.

We now examine the possible exceptions.

If $q = 2$, then $k_0 = 1$ and $\alpha \equiv 1 \pmod 2$ and β satisfies $Bx^2 - (A^2 - 2B)x + B = 0$. Thus $\beta \equiv 1 \pmod{2\,\mathfrak{q}}$ iff $A^2 \equiv 4B \equiv 4 \pmod 8$. Otherwise $\beta \equiv -1 \pmod 4$ and the sequence will not be uniformly distributed modulo 4.

If $q = 3$, we write $\beta^k = 1 + x$ with $x \in \mathfrak{q}$. Then $\beta^{3k} \equiv 1 + (3 + x^2)x$, and $(\beta^{3k} - 1)/(\beta - 1) \equiv 3 + x^2 \pmod{3\mathfrak{q}}$. The only failure occurs when $x^2 \equiv -3 \pmod{3\,\mathfrak{q}}$. In this case we would fail to get uniform distribution modulo 9. Any other case will give uniform distribution modulo all powers of 3.

Conclusion.

Theorem. *The sequence $\langle G_n \rangle$ is uniformly distributed modulo m iff it is uniformly distributed modulo all prime power factors of m. If $\langle G_n \rangle$ is uniformly distributed modulo p (as determined by Propositions* 1 *or* 2) *then $\langle G_n \rangle$ is uniformly distributed modulo p^h with $h > 1$ iff*: (i) $p > 3$; (ii) $p = 3$ *and* $A^2 \not\equiv B \pmod 9$; *or* (iii) $p = 2$, $A \equiv 2 \pmod 4$, $B \equiv 1 \pmod 4$.

Proof. We have seen that only the step from uniform distribution modulo $m_0 q$ to uniform distribution modulo $m_0 q^2$ can fail, and then only for $q = 3$, $((\alpha'/\alpha) - 1)^2 \equiv -3 \pmod{3\mathfrak{q}}$ or $q = 2$ in some cases. The stated conditions are simply translations of these conditions into properties of A and B.

Example 3. $A = 3$, $B = -1$. Thus $A^2 - 4B = 13$. A modulus of uniform distribution must be a power of 13. From Proposition 2, 13 is such a modulus if $G_1 \not\equiv 8G_0 \pmod{13}$. From the Theorem, all powers of 13 will then be moduli of uniform distribution. This was noted as being beyond the methods of [1] with $G_0 = 1$ and $G_1 = 1$, 3, or 5.

Example 4. $A = 8$, $B = 1$. Now $A^2 - 4B = 60$; primes dividing $A^2 - 4B$ are 2, 3 and 5. From Proposition 2 and the Theorem we find:

(i) Uniform distribution modulo 2 if $G_0 + G_1$ odd; not uniformly distributed modulo 4;

(ii) Uniform modulo 3 if $3 \nmid G_0 - G_1$; not uniform modulo 9;

(iii) Uniform modulo 5^h for all h if $5 \nmid G_0 + G_1$. Thus

(a) $G_0 = 1$, $G_1 = 4$ uniform modulo 2 only,

(b) $G_0 = 3$, $G_1 = 7$ uniform modulo 3 only,

(c) $G_0 = 2$, $G_1 = 3$ uniform modulo 6,

(d) $G_0 = 1$, $G_1 = 1$ uniform modulo 5^b.

Parallel efforts. The problems left unsolved in [1] have attracted a great deal of attention. Papers which have come to the author's attention are:

(a) M. B. Nathanson, *Linear recurrences and uniform distribution*, Proc. Amer. Math. Soc. 48 (1975), 289–291.

(b) P. Bundschuh and J. -S. Shiue, *A generalization of a paper by D. D. Wall.*

(c) ———, *Solution of a problem on the uniform distribution of integers.*

(b and c to appear in Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.)

In addition generalization to rings other than Z has been initiated by Kuipers (Abstract 711-10-20, Notices Amer. Math. Soc. 21 (1974), A52). The methods of the present paper should be readily adaptable to that study. It should be noted that the step from uniform distribution modulo m to uniform distribution modulo $m_0 q$ may present difficulties in higher number fields.

REFERENCES

1. L. Kuipers and J. Shiue, *A distribution property of a linear recurrence of the second order*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 52 (1972), 6–10.

2. ———, *A distribution property of the sequence of Lucas numbers*, Elem. Math. 27 (1972), 10–11. MR 46 #144.

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEW BRUNSWICK, NEW JERSEY 08903