GENERALIZATION OF A THEOREM OF VÉLEZ ON UNIFORM DISTRIBUTION IN SECOND-ORDER LINEAR RECURRENCES

Lawrence Somer
Department of Mathematics, Catholic University of America, Washington, D.C.
somer@cua.edu

Michal Křížek
Institute of Mathematics, Czech Academy of Sciences, Prague, Czech Republic
krizek@math.cas.cz

Received: 1/25/24, Revised:10/16/24 , Accepted: 12/20/24, Published: 1/17/25

Abstract

We generalize a result by Vélez on second-order linear recurrence sequences that are uniformly distributed modulo a prime power. Vélez showed that if a second-order linear recurrence is uniformly distributed modulo a prime power p^e, then each residue modulo p^e also appears exactly once in a particular finite subsequence of that recurrence. We find more general finite subsequences such that each residue modulo p^e appears exactly r times in that subsequence, where r may be greater than 1.

1. Introduction

Let $(w) = w(a, b)$ denote the sequence satisfying the second-order linear recursion relation

$$w_{n+2}(a, b) = aw_{n+1}(a, b) + bw_n(a, b),$$

where the parameters a and b and the initial terms $w_0(a, b)$ and $w_1(a, b)$ are all integers. Let $D = D(a, b) = a^2 + 4b$ be the discriminant of $w(a, b)$. When the parameters a and b are known, we frequently write $w_n(a, b)$ simply as w_n. We distinguish two special recurrences, the Lucas sequence of the first kind (LSFK) $u(a, b)$ with initial terms $u_0 = 0$ and $u_1 = 1$, and the Lucas sequence of the second kind (LSSK) $v(a, b)$ with initial terms $v_0 = 2$ and $v_1 = a$. Throughout this paper, p will denote a prime and m will denote a positive integer. It was shown in [4, pp. 344–345] that $w(a, b)$ is purely periodic modulo m if $\gcd(m, b) = 1$. From here on, we assume that $\gcd(m, b) = 1$ and $\gcd(p, b) = 1$. The period length of $w(a, b)$

DOI: 10.5281/zenodo.14679256

modulo m, denoted by $\lambda_w(m)$, is the least positive integer ℓ such that

$$w_{n+\ell} \equiv w_n \pmod{m} \quad \text{for all } n \geq 0.$$

If the recurrence $w(a, b)$ is understood, we will write $\lambda_w(m)$ simply as $\lambda(m)$. The restricted period of $w(a, b)$ modulo m, denoted by $h_w(m)$, is the least positive integer f such that

$$w_{n+f} \equiv M w_n \pmod{m} \quad \text{for all } n \geq 0, \tag{1.1}$$

for some fixed residue M modulo m such that $\gcd(M, m) = 1$. Here, $M = M_w(m)$ is called the *multiplier of* $w(a, b)$ modulo m. Since the LSFK $u(a, b)$ is purely periodic modulo m and has initial term $u_0 = 0$, it is easily seen that $h_u(m)$ is the least positive integer t such that

$$u_t \equiv 0 \pmod{m}.$$

We easily observe that if $\lambda_w(m) \mid r$ and $h_w(m) \mid s$, then r is a general period of $w(a, b)$ modulo m and s is a general restricted period of $w(a, b)$ modulo m. It is proven in [4, pp. 354–355] that $h_w(m) \mid \lambda_w(m)$. Let

$$E_w(m) = \frac{\lambda_w(m)}{h_w(m)}.$$

Then by [4, pp. 354–355], $E_w(m)$ is the multiplicative order of the multiplier $M_w(m)$ modulo m. By repeated applications of (1.1), we see that if $h = h_w(m)$, then

$$w_{n+hi} \equiv M^i w_n \pmod{m} \tag{1.2}$$

for all $n \geq 0$ and $i \geq 1$.

The recurrence $w(a, b)$ is said to be *uniformly distributed* (u. d.) modulo m if each residue modulo m appears exactly the same number of times E in a least period of $w(a, b)$ modulo m, where $E \geq 1$. In 1975, Bumby [1] and Webb and Long [12] independently gave necessary and sufficient criteria for the recurrence $w(a, b)$ to be u. d. modulo m. These criteria will be presented in Theorem 2.3 in Section 2. In [11], Vélez sharpened the results of Bumby and Webb and Long, by showing that if $w(a, b)$ is u. d. modulo p^e, then there exist subsequences of $w(a, b)$ that are also u. d. modulo p^e. Vélez's result is given below.

Theorem 1.1. (Vélez) *Suppose that the sequence $w(a, b)$ is uniformly distributed modulo p^e with period $\lambda_w(p^e) = p^e E$, where $e \geq 1$ and each residue modulo p^e appears exactly E times in a least period of $w(a, b)$ modulo p^e. Let s be a fixed nonnegative integer and define $\{w'_n\}_{n=0}^{\infty}$ by $w'_n = w_{s+nE}(a, b)$. Then each residue modulo p^e appears exactly once in the finite sequence $\{w'_n\}_{n=0}^{p^e-1}$. Moreover, if $p \geq 3$, then $a \not\equiv 0 \pmod{p}$ and $E = \text{ord}_p(a/2)$, while $E = 1$ if $p = 2$.*

We note that already in 1975, twelve years before Vélez's paper, Bumby [1] gave a more precise result than that of Theorem 1.1 above for the case in which $e = 1$.

Theorem 1.2. (Bumby) *Let the sequence $w(a,b)$ be uniformly distributed modulo p with period $\lambda_w(p) = pE$, where each residue modulo p appears exactly E times in a least period of $w(a,b)$ modulo p. Let c be any multiple of E such that $\gcd(c,p) = 1$. Then for every nonnegative integer s, the sequence $w_s, w_{s+c}, \ldots, w_{s+(p-1)c}$ is congruent to an arithmetic progression with nonzero difference modulo p.*

Our main result, which is given below, generalizes Theorem 1.1. The proof of Theorem 1.3 will be given in Section 3 and is shorter than the proof of Theorem 1.1 given by Vélez in [11].

Theorem 1.3. *Suppose that the sequence $w(a,b)$ is uniformly distributed modulo p^e with period $\lambda_w(p^e) = p^e E$, where $\gcd(b,p) = 1$, $e \geq 1$, and each residue modulo p^e appears exactly E times in a least period of $w(a,b)$ modulo p^e. Let g be any fixed positive integer such that $\gcd(g,p) = 1$. Let $d = \gcd(g,E)$ and let $r = \frac{E}{d}$. Let s be a fixed nonnegative integer and define $\{w'_n\}_{n=0}^{\infty}$ by $w'_n = w_{s+ng}(a,b)$. Then each residue modulo p^e appears exactly r times in the finite sequence $\{w'_n\}_{n=0}^{p^e r-1}$. Further, if $p \geq 3$, then $a \not\equiv 0 \pmod{p}$ and $E = \mathrm{ord}_p(a/2)$, while $E = 1$ if $p = 2$.*

2. Auxiliary Results

Before proving our principal result, Theorem 1.3, we introduce some definitions and useful statements. Associated with the recurrence $w(a,b)$ is the characteristic polynomial

$$f(x) = x^2 - ax - b$$

with characteristic roots $\alpha = (a + \sqrt{a^2+4b})/2$, $\beta = (a - \sqrt{a^2+4b})/2$, and discriminant $D = D(a,b) = (\alpha-\beta)^2 = a^2 + 4b$. We will frequently consider the case in which $p \mid D$ for some prime p. In that case, $\alpha \equiv \beta \equiv a/2 \pmod{p}$ if p is odd. We further note that if $p = 2$ and $p \mid D$, then a is even. By the Binet formulas,

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad v_n = \alpha^n + \beta^n, \quad \text{if } D \neq 0,$$

while

$$u_n = n\alpha^{n-1}, \quad v_n = 2\alpha^n, \quad \text{if } D = 0.$$

More generally,

$$w_n = c_\alpha \alpha^n + c_\beta \beta^n \quad \text{if } D \neq 0,$$

where

$$c_\alpha = \frac{w_1 - \beta w_0}{\alpha - \beta}, \quad c_\beta = \frac{\alpha w_0 - w_1}{\alpha - \beta},$$

(see [5, p. 174]), while

$$w_n = (c_1 n + c_2)\alpha^n \quad \text{if } D = 0,$$

where

$$c_1 = \frac{w_1 - w_0\alpha}{\alpha}, \quad c_2 = w_0,$$

(see [9, pp. 33–35]).

A recurrence $w(a, b)$ is called *regular modulo* p, or p-*regular* for short, if

$$\begin{vmatrix} w_0 & w_1 \\ w_1 & w_2 \end{vmatrix} = w_0w_2 - w_1^2 \not\equiv 0 \pmod{p}.$$

Remark 2.1. If $w(a, b)$ is not p-regular, then it is said to be p-*irregular*. It is clear that $w(a, b)$ is p-regular if and only if the vectors (w_0, w_1) and (w_1, w_2) are linearly independent modulo p. Further, $w(a, b)$ is p-irregular precisely when $w(a, b)$ satisfies a recursion relation modulo p of order less than two. Clearly, $w(a, b)$ is p-irregular if $p \mid \gcd(w_0, w_1)$. We note that for the LSFK $u(a, b)$,

$$u_0u_2 - u_1^2 = 0 \cdot a - 1^2 = -1 \not\equiv 0 \pmod{p},$$

while for the LSSK $v(a, b)$,

$$v_0v_2 - v_1^2 = 2(a^2 + 2b) - a^2 = a^2 + 4b = D(a, b).$$

Thus, $u(a, b)$ is always p-regular, while $v(a, b)$ is p-irregular if and only if $p \mid D(a, b)$.

Lemma 2.2 below, which is proved in [2, p. 695], characterizes those sequences $w(a, b)$ that are p-irregular in the case in which $w_0 \not\equiv 0 \pmod{p}$.

Lemma 2.2. *Consider the sequences* $w(a, b)$ *and* $w'(a, b)$ *with discriminant* D *and characteristic roots* α *and* β. *Suppose that* $p \nmid b$. *Then the following hold:*

(i) *If* $w_0 \equiv 0 \pmod{p}$, *then* $w(a, b)$ *is* p-*irregular if and only if* $w_1 \equiv 0 \pmod{p}$.

(ii) *Suppose that* p *is odd,* $p \nmid \gcd(w_0, w_1)$, *and* $(D/p) = -1$, *where* (D/p) *denotes the Legendre symbol and* $(D/p) = 0$ *if* $p \mid D$. *Then* $w(a, b)$ *is* p-*regular.*

(iii) *Suppose that* p *is odd,* $p \nmid \gcd(w_0, w_1)$, *and* $(D/p) = 1$. *Then* α *and* β *lie in* $\mathbb{Z}/p\mathbb{Z}$ *and* $\alpha\beta = -b \not\equiv 0 \pmod{p}$. *Moreover,* $w(a, b)$ *is* p-*irregular if and only if either* $w_1 \equiv \alpha w_0$ *or* $w_1 \equiv \beta w_0 \pmod{p}$. *If* $w_1 \equiv \alpha w_0 \pmod{p}$, *then* $w_n \equiv \alpha^n w_0$ *for* $n \geq 0$. *If* $w_1 \equiv \beta w_0 \pmod{p}$, *then* $w_n \equiv \beta^n w_0$ *for* $n \geq 0$.

(iv) *Suppose that* p *is odd,* $p \nmid \gcd(w_0, w_1)$, *and* $p \mid D$. *Then* $\alpha \equiv \beta \equiv a/2 \pmod{p}$ *and* $a \not\equiv 0 \pmod{p}$. *Furthermore,* $w(a, b)$ *is* p-*irregular if and only if* $w_1 \equiv (a/2)w_0 \pmod{p}$, *in which case* $w_n \equiv (a/2)^n w_0$ *for* $n \geq 0$.

(v) *Suppose that* $p = 2$ *and* $2 \nmid \gcd(w_0, w_1)$. *Then* $w(a, b)$ *is* 2-*irregular if and only if* $a \equiv 0 \pmod{2}$, $b \equiv 1 \pmod{2}$, *and* $w_0 \equiv w_1 \equiv 1 \pmod{2}$, *in which case* $2 \mid D$ *and* $w_n \equiv 1 \pmod{2}$ *for* $n \geq 0$.

(vi) *If $w(a, b)$ is p-irregular, then either $w_n \equiv 0 \pmod{p}$ for all $n \geq 0$ or $w_n \not\equiv 0 \pmod{p}$ for all $n \geq 0$. In particular, if there exists terms w_i and w_j such that $i \neq j$, $w_i \equiv 0 \pmod{p}$, and $w_j \not\equiv 0 \pmod{p}$, then $w(a, b)$ is p-regular.*

(vii) *If $(w) = w(a, b)$ and $(w') = w'(a, b)$ are both p-regular and $e \geq 1$, then $\lambda_w(p^e) = \lambda_{w'}(p^e)$, $h_w(p^e) = h_{w'}(p^e)$, $M_w(p^e) \equiv M_{w'}(p^e) \pmod{p^e}$, and $E_w(p^e) = E_{w'}(p^e)$.*

Proof. All parts except part (vi) follow from results in [2, p. 695]. Part (vi) follows from parts (i)–(v). □

Theorem 2.3. *Let $w(a, b)$ be a recurrence modulo p^e with characteristic roots α and β and discriminant $D = (\alpha - \beta)^2 = a^2 + 4b$. Then the following hold.*

(i) *The recurrence $w(a, b)$ is u. d. modulo p if and only if $p \mid D$ and $w(a, b)$ is regular modulo p. In this case, $h(p) = p$, $\lambda(p) = pE(p)$, and each residue modulo p appears exactly $E(p)$ times in a least period of $w(a, b)$ modulo p. If $p \geq 3$ and $w(a, b)$ is u. d. modulo p, then $a \not\equiv 0 \pmod{p}$, $\alpha \equiv \beta \equiv a/2 \pmod{p}$, and $E(p) = \operatorname{ord}_p(M_w(p)) = \operatorname{ord}_p(\alpha) = \operatorname{ord}_p(a/2)$. If $p = 2$, then $E(p) = 1$. In all cases, $E(p) \mid p - 1$.*

(ii) *Suppose that $p \geq 5$ and $e \geq 2$. Then $w(a, b)$ is u. d. modulo p^e if and only if $p \mid D$ and $w(a, b)$ is regular modulo p. In this case, $a \not\equiv 0 \pmod{p}$, $h(p^e) = p^e$, $E(p) = \operatorname{ord}_p(a/2)$, and $\lambda(p^e) = p^e E(p)$. Moreover, each residue modulo p^e appears exactly $E(p)$ times in a least period of $w(a, b)$ modulo p^e. Further, $E(p) \mid p - 1$.*

(iii) *Suppose that $p = 3$ and $e \geq 2$. Then $w(a, b)$ is u. d. modulo 3^e if and only if $3 \mid D$, $D \not\equiv 6 \pmod{9}$, and $w(a, b)$ is regular modulo 3. In this case, $a \not\equiv 0 \pmod{3}$, $h(3^e) = 3^e$, $E(3) = \operatorname{ord}_3(a/2)$, and $\lambda(3^e) = 3^e E(3)$. Moreover, each residue modulo 3^e appears exactly $E(3)$ times in a least period of $w(a, b)$ modulo 3^e. Furthermore, $E(3) \mid 2$.*

(iv) *Suppose that $p = 2$ and $e \geq 2$. Then $w(a, b)$ is u. d. modulo 2^e if and only if $2 \mid D$, $a \equiv 2 \pmod{4}$, $b \equiv 3 \pmod{4}$, $w_0 \not\equiv w_1 \pmod{2}$, and $w(a, b)$ is regular modulo 2. In this case, $h(2^e) = 2^e$, $E(2) = 1$, and $\lambda(2^e) = 2^e$. Moreover, each residue modulo 2^e appears exactly once in a least period of $w(a, b)$ modulo 2^e.*

(v) *If $p \geq 3$ and $p \mid D$, then $w(a, b)$ is regular modulo p if and only if $p \nmid 2w_1 - w_0$. If $p = 2$ and $p \mid D$, then $a \equiv 0 \pmod{2}$ and $w(a, b)$ is regular modulo 2 if and only if $w_0 \not\equiv w_1 \pmod{2}$.*

Proof. This follows from Lemma 2.2 (iv) and (v) of this paper and results in [1], [12], [8], [11, p. 38], Theorem 1.11 of [6], and [7, pp. 30–48]. □

Theorem 2.4 below will be needed to prove Theorem 1.3.

Theorem 2.4. *Let $w(a,b)$ be any second-order linear recurrence and define w'_n by $w'_n = w_{tn+r}(a,b)$, where $n \geq 0$, t is a fixed positive integer, and r is a fixed nonnegative integer. Then for all $n \geq 0$,*

$$w'_{n+2} = a'w'_{n+1} + b'w'_n,$$

where $a' = v_t(a,b)$ and $b' = (-1)^{t+1}b^t$, and the sequence $\{w'_n\}_{n=0}^{\infty}$ is equal to the second-order recurrence sequence $w(a',b')$. Further, if α and β are the characteristic roots of $w(a,b)$ and $D(a,b)$ is the discriminant of $w(a,b)$, then $w(a',b')$ has characteristic roots α^t and β^t and discriminant $D(a',b') = (u_t(a,b))^2 D(a,b)$.

Proof. All assertions of Theorem 2.4 follow from [10], except for the one concerning the discriminant of $w(a',b')$. We note that

$$D(a',b') = (\alpha^t - \beta^t)^2 = \Big(\frac{\alpha^t - \beta^t}{\alpha - \beta}\Big)^2 (\alpha-\beta)^2 = (u_t(a,b))^2 D(a,b).$$

□

3. Proof of the Main Theorem

We are now able to prove Theorem 1.3.

Proof of Theorem 1.3. Let $(w) = w(a,b)$ with characteristic roots α and β and discriminant $D = D(a,b)$. Since (w) is u. d. modulo p^e, we see by Theorem 2.3 that $p \mid D$, (w) is p-regular, $h = h_w(p) = p$, $E = E_w(p) = \mathrm{ord}_p(\alpha) = \mathrm{ord}_p(a/2)$, and $\lambda_w(p^e) = p^e E$. Further, each residue modulo p^e appears exactly E times in a least period of (w) modulo p^e. Moreover, there exists a nonnegative integer ℓ such that $0 \leq \ell \leq h-1 = p-1$ and $w_\ell \equiv 0 \pmod{p}$. Then $w_n(a,b) \equiv 0 \pmod{p}$ if and only if $n \equiv \ell \pmod{p}$.

We define the sequence $\{w'_n\}_{n=0}^{\infty}$ by $w'_n = w_{s+ng}(a,b)$. Then by Theorem 2.4, $\{w'_n\}_{n=0}^{\infty} = (w') = w(a',b')$, where $a' = v_g(a,b)$ and $b' = (-1)^{g+1}b^g$. Additionally, by Theorem 2.4, (w') has characteristic roots α^g and β^g and discriminant

$$D' = D(a',b') = (u_g(a,b))^2 D.$$

Since $\gcd(b,p) = 1$ and $p \mid D$, we see that $\gcd(b',p) = 1$ and $p \mid D'$. We will show below that $(w') = w(a',b')$ is u. d. modulo p^e and $E' = E_{w'}(p) = r$. Then by Theorem 2.3, it would follow that $\lambda_{w'}(p^e) = p^e r$ and each residue modulo p^e appears exactly r times in a least period of $(w') = w(a',b')$, as desired.

We first show that $(w') = w(a',b')$ is p-regular. Consider the first $h = p$ terms

$$w_s(a,b),\ w_{s+g}(a,b), \ldots, w_{s+(p-1)g}(a,b)$$

of $w(a', b')$. Since $\gcd(g, p) = 1$, it follows that the set $\{s, s+g, \ldots, s+(p-1)g\}$ is congruent to the set $\{0, 1, \ldots, p-1\}$ modulo p. Thus, $w_{s+ig}(a, b) \equiv 0 \pmod{p}$ if and only $i \equiv \ell \pmod{p}$, where $0 \le i \le p-1$. Hence, there are terms w'_i and w'_j such that $w'_i \equiv 0 \pmod{p}$ and $w'_j \not\equiv 0 \pmod{p}$. It now follows by Lemma 2.2 (vi) that $w(a', b')$ is p-regular. It further follows by Theorem 2.3 (i) and (ii) that $w(a', b')$ is u. d. modulo p^e if either $e = 1$ or it is the case that $e \ge 2$ and $p \ge 5$.

We now suppose that $p = 3$ and $e \ge 2$. Then $3 \mid D$ and $D \not\equiv 6 \pmod{9}$ by Theorem 2.3 (iii), since $w(a, b)$ is u. d. modulo 3^e. By Theorem 2.4,

$$D' = D(a', b') = (u_g(a, b))^2 D.$$

By inspection, $(u_g(a, b))^2 \equiv 0, 1, 4$, or $7 \pmod{9}$, while $D \equiv 0$ or $3 \pmod{9}$. By examination, we then observe that $D' = (u_g(a, b))^2 D \equiv 0$ or $3 \pmod{9}$, and also $D' \not\equiv 6 \pmod{9}$. Consequently, $w(a', b')$ is u. d. modulo 3^e by Theorem 2.3 (iii).

We next suppose that $p = 2$ and $e \ge 2$. Then $g \equiv 1 \pmod{2}$, since $\gcd(g, 2) = 1$. Moreover, $a \equiv 2 \pmod{4}$, $b \equiv 3 \pmod{4}$, and $w_0(a, b) \not\equiv w_1(a, b) \pmod{2}$ by Theorem 2.3 (iv). Since $a \equiv 0 \pmod{2}$ and $b \equiv 1 \pmod{2}$, we can find that $w_{2i}(a, b) \equiv w_0(a, b) \pmod{2}$ and $w_{2i+1}(a, b) \equiv w_1(a, b) \pmod{2}$ for $i \ge 0$. By Theorem 2.1, $a' = v_g(a, b)$ and $b' = (-1)^{g+1} b^g \equiv 1 \cdot 3^g \equiv 3 \pmod{4}$. Noting that $v_0(a, b) = 2$ and $v_1(a, b) = a \equiv 2 \pmod{4}$, it follows now by induction that $v_n(a, b) \equiv 2 \pmod{4}$ for all $n \ge 0$. Hence, $a' \equiv 2 \pmod{4}$ and $b' \equiv 3 \mod 4$. We now show that $w_1(a', b') \not\equiv w_0(a', b')$. By definition, $w_0(a', b') = w_s(a, b)$ and $w_1(a', b') = w_{s+g}(a, b)$, where $\gcd(g, 2) = 1$. Then $s \not\equiv s + g \pmod{2}$, which implies that $w_1(a', b') \not\equiv w_0(a', b') \pmod{2}$. Hence, $w(a', b')$ is u. d. modulo 2^e by Theorem 2.3 (iv).

Finally, we show that $\lambda_{w'}(p^e) = p^e r$, which then implies that each residue modulo p^e appears exactly r times in a least period of $w(a', b')$ modulo p^e, because $w(a', b')$ is u. d. modulo p^e. By Theorem 2.3 (i) and (ii), $\lambda_{w'}(p^e) = p^e E_{w'}(p)$. It thus suffices to show that $E_{w'}(p) = r$. By our earlier arguments, $w(a', b')$ has characteristic roots α^g and β^g and $E_{w'}(p) = \operatorname{ord}_p(\alpha^g)$. Since $E_w(p) = \operatorname{ord}_p(\alpha)$ by our above discussion, we see that

$$E_{w'}(p) = \operatorname{ord}_p(\alpha^g) = \frac{E_w(p)}{\gcd(E_w(p), g)} = r.$$

Our result now follows. □

4. Conclusions

Remark 4.1. We observe that in a certain sense, Theorem 1.3 is the best possible. Let g be any fixed positive integer. Let s be a fixed nonnegative integer and define $\{w'_n\}_{n=0}^{\infty}$ by $w'_n = w_{s+ng}(a, b)$. Suppose that $\gcd(g, p) > 1$. Let $g = pi$ for some positive integer i. We claim that the finite subsequence $\{w'_n\}_{n=0}^{p^e r-1}$ does not contain all residues modulo p^e, where $e \geq 1$. By Theorem 2.3 (i), $h(p) = p$. It now follows by (1.2) that

$$w'_n = w_{s+ng} \equiv M^{ni} w_s \pmod{p} \tag{4.1}$$

for $n \in \{0, 1, \dots, p^e r - 1\}$, where $M = M(p)$. Since $\gcd(M, p) = 1$, we see by (4.1) that $w'_n \not\equiv 0 \pmod{p}$ if $w_s \not\equiv 0 \pmod{p}$, while $w'_n \equiv 0 \pmod{p}$ if $w_s \equiv 0 \pmod{p}$.

We now consider the problem of extending our results from second-order linear recurrence sequences to kth-order linear recurrence sequences, where $k \geq 2$. Let $w(a_1, a_2, \dots, a_k)$ denote the kth-order linear recurrence defined by

$$w_{n+k} = a_1 w_{n+k-1} + a_2 w_{n+k-2} + \cdots + a_k w_n,$$

where the parameters $a_1, a_2, \dots, a_k$ and the initial terms $w_0, w_1, \dots, w_{k-1}$ are all integers. Let

$$g(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_{k-1} x - a_k$$

be the characteristic polynomial of $w(a_1, a_2, \dots a_k)$ with roots $\alpha_1, \alpha_2, \dots, \alpha_k$ and discriminant

$$D = \prod_{1 \leq i < j \leq k} (\alpha_i - \alpha_j)^2.$$

We make the following conjecture.

Conjecture 4.2. Suppose that the sequence $w(a_1, a_2, \dots, a_k)$ is uniformly distributed modulo p^e with period $\lambda_w(p^e) = p^e E$, where $\gcd(a_k, p) = 1$, $e \geq 1$, and each residue modulo p^e appears exactly E times in a least period of $w(a_1, a_2, \dots, a_k)$ modulo p^e. Let g be any fixed positive integer such that $\gcd(g, p) = 1$. Let $d = \gcd(g, E)$ and let $r = \frac{E}{d}$. Let s be a fixed nonnegative integer and define $\{w'_n\}_{n=0}^{\infty}$ by $w'_n = w_{s+ng}(a_1, a_2, \dots, a_k)$. Then each residue modulo p^e appears exactly r times in the finite sequence $\{w'_n\}_{n=0}^{p^e r - 1}$.

The example below provides some justification for Conjecture 4.2.

Example 4.3. Consider the third-order linear recurrence $(w) = w(3, -1, -2)$ defined by

$$w_{n+3} = 3w_{n+2} - w_{n+1} - 2w_n,$$

with initial terms $w_0 = 0$, $w_1 = 0$, $w_2 = 1$, and having the characteristic polynomial

$$f(x) = x^3 - 3x^2 + x + 2$$

with characteristic roots $\alpha_1 = (1+\sqrt{5})/2$, $\alpha_2 = (1-\sqrt{5})/2$, $\alpha_3 = 2$, and discriminant $D = 5$. By inspection, (w) is u. d. modulo 25 with period $\lambda(25) = 100 = 25 \cdot 4$. Let g be a fixed positive integer such that $\gcd(g, 5) = 1$. Let

$$r = \frac{4}{\gcd(4, g)}$$

Consider the finite subsequence of (w) defined by

$$w_0, w_g, w_{2g}, \dots w_{(25r-1)g}. \tag{4.2}$$

By examination, the subsequence (4.2) is u. d. with each residue modulo 25 appearing exactly r times when $(g, r) = (4, 1)$ or $(2, 2)$ or $(3, 4)$.

Acknowledgments. We thank the anonymous referee for suggestions which improved the content and exposition of the paper. This paper was supported by RVO 67985840 of the Czech Academy of Sciences.

References

[1] R. T. Bumby, A distribution property for linear recurrences of the second order, *Proc. Amer. Math. Soc.* **50** (1975), 101-106.

[2] W. Carlip and L. Somer, Bounds for frequencies of residues of regular second-order recurrences modulo p^r, in *Number Theory in Progress, Vol. 2*, (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 691-719.

[3] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913), 30-70.

[4] R. D. Carmichael, On sequences of integers defined by recurrence relations, *Quart. J. Pure Appl. Math.* **48** (1920), 343-372.

[5] D. Kalman and R. Mena, The Fibonacci numbers exposed, *Math. Mag.* **76** (2003), 167-181.

[6] D. H. Lehmer, An extended theory of Lucas' functions, *Ann. of Math.* **31** (1930), 419-448.

[7] W. Narkiewicz, Uniform distribution of sequences of integers in residue classes, *Lecture Notes in Mathematics 1087*, Springer, Berlin, 1984.

[8] M. B. Nathanson, Linear recurrences and uniform distribution, *Proc. Amer. Math. Soc.* **48** (1975), 289-291.

[9] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge, 1986.

[10] L. Somer, Solution to Problem H-377, *Fibonacci Quart.* **24.3** (1986), 284-285.

[11] W. Y. Vélez, Uniform distribution of two-term recurrence sequences, *Trans. Amer. Math. Soc.* **301** (1987), 37-45.

[12] W. A. Webb and C. T. Long, Distribution modulo p^h of the general linear second order recurrence, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* **58** (8) (1975), 92-100.