DISTRIBUTION OF RESIDUES OF CERTAIN SECOND-ORDER LINEAR RECURRENCES MODULO p—II

Lawrence Somer
Catholic University of America, Washington, D.C. 20064
(Submitted March 1989)

1. Introduction

Let $(u) = u(a, b)$, called the Lucas sequence of the first kind (LSFK), be a second-order linear recurrence satisfying the relation

(1) $\quad u_{n+2} = au_{n+1} + bu_n,$

where $u_0 = 0$, $u_1 = 1$, and the parameters a and b are integers. Let $D = a^2 + 4b$ be the discriminant of $u(a, b)$. Let $(v) = v(a, b)$, called the Lucas sequence of the second kind (LSSK), be a recurrence satisfying (1) with initial terms $v_0 = 2$, $v_1 = a$. Throughout this paper, p will denote an odd prime unless specified otherwise. Further, d will always denote a residue modulo p. The *period* of $u(a, b)$ modulo p will be denoted by $\mu(p)$. It is known (see [5]) that, if $p \nmid b$, then $u(a, b)$ is purely periodic modulo p. We will always assume that, in the LSFK $u(a, b)$, $p \nmid b$. The *restricted period* of $u(a, b)$ modulo p, denoted by $\alpha(p)$, is the least positive integer t such that $u_{n+t} \equiv su_n \pmod p$ for all nonnegative integers n and some nonzero residue s. Then s is called the *principal multiplier* of (u) modulo p. It is easy to see that $\alpha(p) \mid \mu(p)$ and that $\beta(p) = \mu(p)/\alpha(p)$ is the exponent of the principal multiplier s of (u) modulo p.

We will let $A(d)$ denote the number of times the residue d appears in a full period of $u(a, b)$ modulo p and $N(p)$ denote the number of distinct residues appearing in $u(a, b)$ modulo p. In a previous paper [13], the author considered the LSFK $u(a, 1)$ modulo p and gave constraints for the values which $A(d)$ can attain. In particular, it was shown that $A(d) \le 4$ for all d. Upper and lower bounds for $N(p)$ were given in terms of $\alpha(p)$. Schinzel [8] improved on the constraints given in [13] for the values $A(d)$ can have in the LSFK $u(a, 1)$ modulo p.

In this paper we will consider the LSFK $u(a, -1)$ modulo p and determine the possible values for $A(d)$. In particular, we will show that $A(d) \le 2$ for all d. We will also obtain upper bounds for $N(p)$. If $\alpha(p)$ is known, we will determine $N(p)$ exactly. Schinzel [8] also presented results concerning $A(d)$ for the LSFK $u(a, -1) \pmod p$, citing a preprint on which the present paper is based.

In [12], the author obtained the following partial results concerning $A(d)$ in the LSFK $u(a, -1) \pmod p$.

Theorem 1: Consider the LSFK $u(a, -1)$ modulo p with discriminant $D = a^2 - 4$.

(i) If $p \ge 5$ and $p \nmid D$, then there exists a residue d such that $A(d) = 0$.

(ii) If $p \mid D$, then $A(d) \ne 0$ for any d. In particular, we must have that $a \equiv \pm 2 \pmod p$. If $a \equiv 2 \pmod p$, then

$$u_n \equiv n \pmod p$$

and $A(d) = 1$ for all d. If $a \equiv -2 \pmod p$, then

$$u_n \equiv (-1)^{n+1} n \pmod p$$

and $A(d) = 2$ for all d.

2. Preliminaries

A *general multiplier* of $u(a, b)$ (mod p) is any nonzero residue s' such that

$$u_{n+t} \equiv s'u_n \pmod{p}$$

for some fixed positive integer t' and all nonzero integers n. It is known that, if s is the principal multiplier of $u(a, b)$ (mod p) and s' is a general multiplier of $u(a, b)$ (mod p), then

$$s' \equiv s^i \pmod{p}$$

for some i such that $0 \le i \le \beta(p) - 1$.

For the LSFK $u(a, b)$, let $k = \alpha(p)$. We will let $A_i(d)$ denote the number of times the residue d appears among the terms

$$u_{ki},\ u_{ki+1},\ \ldots,\ u_{ki+k-1} \text{ modulo } p,$$

where $0 \le i \le \beta(p) - 1$. Results concerning $A_i(d)$ will be obtained for the LSFK $u(a, -1)$ (mod p).

The following results concerning $u(a, b)$ and $v(a, b)$ are well known:

$$v_n^2 - Du_n^2 = 4(-b)^n; \tag{2}$$

$$u_{2n} = u_n v_n. \tag{3}$$

Proofs can be found in [4].

3. The Main Theorems

Our results concerning the distribution of residues in the LSFK $u(a, -1)$ modulo p will depend on knowledge of the values of $\alpha(p)$, $\beta(p)$, and (D/p), where (D/p) denotes the Legendre symbol. Theorems 2 and 3 will provide information on the values $\mu(p)$, $\alpha(p)$, and $\beta(p)$ can take for the LSFK $u(a, -1)$ depending on whether $(D/p) = 0$, 1, or -1.

Theorem 2: Let $u(a, b)$ be a LSFK. Then

$$\alpha(p) \mid p - (D/p). \tag{4}$$

Further, if $p \nmid D$, then

$$\alpha(p) \mid (p - (D/p))/2 \tag{5}$$

if and only if $(-b/p) = 1$. Moreover, if $(D/p) = 1$, then

$$\mu(p) \mid p - 1. \tag{6}$$

Proof: Proofs of (4) and (6) are given in [4, pp. 44-45] and [1, pp. 315-17]. Proofs of (5) are given in [6, p. 441] and [1, pp. 318-19].

Theorem 3: Consider the LSFK $u(a, -1)$ with discriminant D. Suppose that $p \nmid D$. Let D' be the square-free part of D. If $|a| \ge 3$, let ε be the funcamental unit of $Q(\sqrt{D'})$. Let s be the principal multiplier of $u(a, -1)$ modulo p.

(i) $\beta(p) = 1$ or 2; $s \equiv 1$ or $-1 \pmod{p}$.
(ii) If $\alpha(p) \equiv 0 \pmod{2}$, then $\beta(p) = 2$.
(iii) If $\alpha(p) \equiv 1 \pmod{2}$, then $\beta(p)$ may be 1 or 2.
(iv) If $(2 - a/p) = (2 + a/p) = -1$, then $\alpha(p) \equiv 0 \pmod{2}$ and $\beta(p) = 2$.
(v) If $(2 - a/p) = 1$ and $(2 + a/p) = -1$, then $\alpha(p) \equiv 1 \pmod{2}$ and $\beta(p) = 2$.
(vi) If $(2 - a/p) = -1$ and $(2 + a/p) = 1$, then $\alpha(p) \equiv 1 \pmod{2}$ and $\beta(p) = 1$.
(vii) If $p \equiv 1 \pmod{4}$, $(D/p) = 1$, and the norm of ε is -1, then $\alpha(p) \mid (p-1)/4$.

Proof: This is proved in [11, pp. 328-31].

We are now ready for the statement of our principal theorems. Following the notation introduced by Schinzel in [8], we will let $S = S(p)$ denote the set of all the values which $A(d)$ attains in the LSFK $u(a, -1)$ modulo p.

Theorem 4: Let $u(a, -1)$ be an LSFK. Suppose that $\beta(p) = 1$, and let $k = \alpha(p)$. Then $k \equiv 1 \pmod 2$. Let $A_0'(d)$ denote the number of times the residue d appears among the terms $u_0, u_1, \ldots, u_{(k-1)/2}$ modulo p. Let $A_1'(d)$ denote the number of times the residue d appears among the terms $u_{(k+1)/2}, u_{(k+3)/2}, \ldots, u_k$ modulo p.

(i) $A(d) = A(-d)$.
(ii) If $p \geq 5$, then $S = \{0, 1\}$.
(iii) $A'(d) = 0$ or 1 for $i = 0, 1$.
(iv) $A_0'(d) = A_1'(-d)$.

Theorem 5: Let $u(a, -1)$ be an LSFK. Suppose that $\alpha(p) \equiv 1 \pmod 2$ and $\beta(p) = 2$.

(i) $A(d) = A(-d)$.
(ii) If $p \geq 5$, then $S = \{0, 2\}$.
(iii) If $d \not\equiv 0 \pmod p$, then $A_i(d) = 0$ or 2 for $i = 0, 1$.
(iv) $A_0(0) = A_1(0) = 1$.
(v) $A_0(d) = A_1(-d)$.

Theorem 6: Let $u(a, -1)$ be an LSFK with discriminant D. Suppose $\alpha(p) \equiv 0 \pmod 2$. Then $\beta(p) = 2$ and $(-D/p) = 1$.

(i) $A(d) = A(-d)$.
(ii) $A(d) = 1$ if and only if $d \equiv \pm 2/\sqrt{-D} \pmod p$.
(iii) If $p \geq 5$, then $S = \{0, 1, 2\}$.
(iv) If $d \not\equiv 0$ or $\pm 2/\sqrt{-D} \pmod p$, then $A_i(d) = 0$ or 2 for $i = 0, 1$.
(v) If $d \equiv 0$ or $\pm 2/\sqrt{-D} \pmod p$, then $A_i(d) = 1$ for $i = 0, 1$.
(vi) $A_0(d) = A_1(-d)$.

Theorem 7: Let $u(a, -1)$ be an LSFK. Suppose that $p \nmid D$ and $a \not\equiv 0, 1$, or $-1 \pmod p$. Let D' be the square-free part of D. Let ε be the fundamental unit of $Q(\sqrt{D'})$. Let $c_1 = 0$ if $\alpha(p) \equiv 1 \pmod 2$ and $c_1 = 1$ if $\alpha(p) \equiv 0 \pmod 2$.

(i) $N(p) \equiv 1 \pmod 2$.
(ii) $N(p) \leq (p - (D/p))/2 + c_1$.
(iii) If $p \equiv 1 \pmod 4$, $(D/p) = 1$, and ε has norm -1, then

$$N(p) \leq (p - 1)/4 + c_1.$$

(iv) $N(p) = \alpha(p) + c_1$.

4. Necessary Lemmas

The following lemmas will be needed for the proofs of Theorems 4-7.

Lemma 1: Let $u(a, b)$ be an LSFK. Let s be the principal multiplier of (u) modulo p and let $k = \alpha(p)$. Then

$$u_{k-n} \equiv (-1)^{n+1} s u_n / b^n \pmod p, \tag{7}$$

for $0 \leq n \leq k$. In particular, if $b \equiv -1 \pmod p$, then

$$u_{k-n} \equiv -s u_n \pmod p, \tag{8}$$

for $0 \leq n \leq k$.

Proof: We proceed by induction. Clearly,

$$u_{k-0} \equiv 0 \equiv (-1)^{0+1} s u_0 / b^0 \equiv 0 \equiv u_0 \pmod p.$$

Also,

$$u_{k-1} \equiv b^{-1}(u_{k+1} - a u_k) \equiv b^{-1}(s u_1 - a \cdot 0) \equiv (-1)^{1+1} s u_1 / b^1 \pmod p.$$

Now assume that

$$u_{k-n} \equiv (-1)^{n+1} s u_n / b^n \pmod{p}$$

and

$$u_{k-(n+1)} \equiv (-1)^{n+2} s u_{n+1} / b^{n+1} \pmod{p}.$$

Then

$$\begin{aligned} u_{k-(n+2)} &\equiv b^{-1}(u_{k-n} - a u_{k-(n+1)}) \\ &\equiv b^{-1}(-1)^{n+1} s[(b u_n / b^{n+1}) + (a u_{n+1} / b^{n+1})] \\ &= b^{-1}(-1)^{n+1} s(u_{n+2}/b^{n+1}) \equiv (-1)^{n+3} s u_{n+2}/b^{n+2} \pmod{p}. \end{aligned}$$

The result for $b \equiv -1 \pmod{p}$ follows by inspection.

Lemma 2: Let $u(a, b)$ be an LSFK. Let n and c be positive integers such that $n + c \le \alpha(p) - 1$. Let $k = \alpha(p)$. Then

$$(9) \qquad (u_{n+c}/u_n)(u_{k-n}/u_{k-n-c}) \equiv (-b)^c \pmod{p}.$$

Proof: This follows from congruence (7) in Lemma 1. Another proof is given in [12, p. 123].

Lemma 3: Consider the LSFK $u(a, b)$. Let c be a fixed integer such that $1 \le c \le \alpha(p) - 1$. Then the ratios u_{n+c}/u_n are all distinct modulo p for $1 \le n \le \alpha(p) - 1$.

Proof: This is proved in [12, pp. 120-21].

Lemma 4: Let $u(a, -1)$ be an LSFK and let $k = \alpha(p)$. Then

$$u_n \not\equiv \pm u_{n+c} \pmod{p}$$

for any positive integers n and c such that either $n + c \le k/2$ or it is the case that $n \ge k/2$ and $n + c \le k - 1$.

Proof: Suppose there exist positive integers n and c such that $n + c \le k - 1$ and

$$u_n \equiv \pm u_{n+c} \pmod{p}.$$

Then

$$u_{n+c}/u_n \equiv \pm 1 \pmod{p}.$$

By Lemma 2,

$$(u_{n+c}/u_n)(u_{k-n}/u_{k-n-c}) \equiv 1^c \equiv 1 \pmod{p};$$

hence,

$$u_{k-n}/u_{k-n-c} \equiv u_{n+c}/u_n \equiv \pm 1 \pmod{p}.$$

Thus, by Lemma 3,

$$n + c = k - n$$

leading to

$$n = (k - c)/2.$$

Consequently,

$$n = (k - c)/2 \text{ and } n + c = (k + c)/2.$$

The result now follows.

Lemma 5: Let $u(a, -1)$ be an LSFK and let $k = \alpha(p)$. Let N_1 be the largest integer t such that there exist integers $n_1, n_2, \ldots, n_t$ for which $1 \le n_i \le [k/2]$ and $u_{n_i} \not\equiv \pm u_{n_j} \pmod{p}$ if $1 \le i < j \le [k/2]$, where $[x]$ is the greatest integer less than or equal to x. Then

$$(10) \qquad N(p) = 2N_1 + 1.$$

Proof: By Theorem 3, $\beta(p) = 1$ or 2. First, suppose that $\beta(p) = 2$. Then -1 is the principal multiplier of (u) modulo p and the residue $-d$ appears in (u)

modulo p if and only if d appears in (u) modulo p. Moreover, it follows from Lemma 1 and the fact that -1 is a principal multiplier of (u) modulo p that if $d \not\equiv 0 \pmod p$ and d appears in $(u) \pmod p$, then $d \equiv \pm u_{n_i} \pmod p$ for some i such that $1 \le i \le N_1$. Including the residue 0, we see that (10) holds.

Now suppose that $\beta(p) = 1$. By congruence (8) in Lemma 1, the residue $-d$ appears in (u) modulo p if and only if d appears in (u) modulo p. It also follows from Lemma 1 that, if $d \not\equiv 0 \pmod p$ and d appears in (u) modulo p, then $d \equiv \pm u_{n_i} \pmod p$ for some i such that $1 \le i \le N_1$. Counting the residue 0, we see that the result follows.

Lemma 6: Let $u(a, -1)$ be an LSFK. Let $k = \alpha(p)$. Let $A'(d)$ denote the number of times the residue d appears among the terms $n_1, n_2, \ldots, n_{[k/2]}$ modulo p. Let N_1 be defined as in Lemma 5.

(i) $A'(d) + A'(-d) = 0$ or 1.
(ii) $N_1 = [k/2]$.

Proof: (i) follows from Lemma 4; (ii) follows from (i).

Lemma 7: Let $u(a, b)$ be an LSFK. Suppose that $p \nmid b$. Let s be the principal multiplier of (u) modulo p and s^j be a general multiplier of $(u) \pmod p$, where $1 \le j \le \beta(p) - 1$. Then

$$A(d) = A(s^j d).$$

Proof: This is proved in [13].

Lemma 8: Let $u(a, -1)$ be an LSFK with discriminant D. Suppose that $\alpha(p) \equiv 0 \pmod 2$. Let $k = \alpha(p)$. Then

$$u_{k/2} \equiv \pm 2/\sqrt{-D} \pmod p.$$

Proof: Since $\alpha(p) \equiv 0 \pmod 2$, it follows from (4) that $p \nmid D$. By (2), it follows that

$$v_{k/2}^2 - Du_{k/2}^2 = 4(1)^{k/2} = 4. \tag{11}$$

Now, $u_{k/2} \not\equiv 0 \pmod p$. Thus, by (3), $v_{k/2} \equiv 0 \pmod p$. Hence, by (11),

$$-Du_{k/2}^2 \equiv 4 \pmod p$$

and the result follows.

5. Proofs of the Main Theorems

We are finally ready to prove Theorems 4-7.

Proof of Theorem 4: The fact that $\alpha(p) \equiv 1 \pmod 2$ follows from Theorem 3.

(i) and (iv) follow from Lemma 1; (ii) follows from Theorem 1(i), Lemma 6(i), and Lemma 1; (iii) follows from Lemma 6(i) and the fact that $A(0) = 1$.

Proof of Theorem 5: (i) follows from Lemma 7; (ii) and (iii) follow from Theorem 1(i), Lemma 6(i), Lemma 1, and the fact that -1 is the principal multiplier of $u(a, -1)$ modulo p; (iv) follows by inspection; and (v) follows from the fact that -1 is the principal multiplier of (u) modulo p.

Proof of Theorem 6: The fact that $\beta(p) = 2$ follows from Theorem 3. The fact that $(-D/p) = 1$ follows from Lemma 8.

(i) follows from Lemma 7; (ii), (iv), and (v) follow from Lemmas 8, 6(i), and 1 and the fact that -1 is the principal multiplier of (u) modulo p; (iii) follows from Theorem 1(i), Lemma 6(i), Lemma 1 and the fact that -1 is the principal multiplier of $u(a, -1)$ modulo p; and (vi) follows from the fact that -1 is the principal multiplier of (u) modulo p.

Remark: Note that Theorem 3 gives conditions for the hypotheses of Theorems 4-6 to be satisfied.

Proof of Theorem 7: (i) follows from Lemma 5; (ii) follows from Lemma 5, Lemma 6(ii), and Theorem 2; (iii) This follows from Lemma 5, Lemma 6(ii), and Theorem 3(vii); and (iv) follows from Lemmas 5 and 6(ii).

6. Special Cases

For completeness, we present Theorems 8 and 9 which detail special cases we have not treated thus far. For these theorems, p will designate a prime, not necessarily odd.

Theorem 8: Let $u(a, -1)$ be an LSFK. Suppose $p \nmid D$.

(i) If $a \equiv 0 \pmod{p}$, then $\alpha(p) = 2$, $\beta(p) = 2$, $N(p) = 3$, $A(0) = 2$, $A(1) = A(-1) = 1$, and $A(d) = 0$ if $d \not\equiv 0, 1$, or $-1 \pmod{p}$.
(ii) If $a \equiv 1 \pmod{p}$ and $p > 2$, then $\alpha(p) = 3$, $\beta(p) = 2$, $N(p) = 3$, $A(0) = A(1) = A(-1) = 2$, and $A(d) = 0$ if $d \not\equiv 0, 1$, or $-1 \pmod{p}$.
(iii) If $a \equiv 1 \pmod{p}$ and $p = 2$, then $\alpha(p) = 3$, $\beta(p) = 1$, $N(p) = 2$, $A(0) = 1$, and $A(1) = 2$.
(iv) If $a \equiv -1 \pmod{p}$ and $p > 2$, then $\alpha(p) = 3$, $\beta(p) = 1$, $N(p) = 3$, $A(0) = A(1) = A(-1) = 1$, and $A(d) = 0$ if $d \not\equiv 0, 1$, or $-1 \pmod{p}$.

Proof: (i)-(iv) follow by inspection.

Theorem 9: Let $u(a, -1)$ be an LSFK. Suppose that $p \mid D$. Then $a \equiv \pm 2 \pmod{p}$. If $a \equiv 2 \pmod{p}$, then $\alpha(p) = p$, $\beta(p) = 1$, $N(p) = p$, and $A(d) = 1$ for all residues d modulo p. If $p > 2$ and $a \equiv -2 \pmod{p}$, then $\alpha(p) = p$, $\beta(p) = 2$, $N(p) = p$, and $A(d) = 2$ for all residues d modulo p.

Proof: This follows from Theorem 1(ii).

Remark: If $D \equiv 0 \pmod{p}$, we see from Theorem 9 that the residues of $u(a, -1)$ are equidistributed modulo p. See [7, p. 463] for a comprehensive list of references on equidistributed linear recurrences.

7. Concluding Remarks

In [8] and [13] it was shown that, for the LSFK $u(a, 1)$ modulo p, $A(d) \le 4$. In the present paper it was shown that, for the LSFK $u(a, -1)$ modulo p, $A(d) \le 2$. In [14] we extend these results considerably. Specifically, let $w(a, b)$ be a second-order linear recurrence with arbitrary initial terms w_0, w_1 over the finite field F_q satisfying the relation

$$w_{n+2} = aw_{n+1} + bw_n.$$

where $b \ne 0$. Then

$$A(d) \le 2 \cdot \operatorname{ord}(-b)$$

for all elements $d \in F_q$, where $\operatorname{ord}(x)$ denotes the order of x in F_q.

References

1. R. P. Backstrom. "On the Determination of the Zeros of the Fibonacci Sequence." *Fibonacci Quarterly* 4.4 (1966):313-22.
2. G. Bruckner. "Fibonacci Sequences Modulo a Prime $p \equiv 3 \pmod{4}$." *Fibonacci Quarterly* 8.2 (1970):217-20.
3. S. A. Burr. "On Moduli for Which the Fibonacci Sequence Contains a Complete System of Residues." *Fibonacci Quarterly* 9.4 (1971):497-504.

4. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Ann. Math. Second Series* *15* (1913):30-70.
5. R. D. Carmichael. "On Sequences of Integers Defined by Recurrence Relations." *Quart. J. Pure Appl. Math.* *48* (1920):343-72.
6. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. Math. Second Series* *31* (1930):419-48.
7. R. Lidl & H. Niederreiter. *Finite Fields*. Reading, Mass.: Addison-Wesley, 1983.
8. A. Schinzel. "Special Lucas Sequences, Including the Fibonacci Sequence, Modulo a Prime." To appear.
9. A. P. Shah. "Fibonacci Sequences Modulo m." *Fibonacci Quarterly* *6.1* (1968):139-41.
10. L. Somer. "The Fibonacci Ratios F_{k+1}/F_k Modulo p." *Fibonacci Quarterly* *13.4* (1975):322-24.
11. L. Somer. "The Divisibility Properties of Primary Lucas Recurrences with Respect to Primes." *Fibonacci Quarterly* *18.4* (1980):316-34.
12. L. Somer. "Primes Having an Incomplete System of Residues for a Class of Second-Order Linear Recurrences." *Applications of Fibonacci Numbers*. Ed. by A. N. Philippou, A. F. Horadam, & G. E. Bergum. Dordrecht, Holland: Kluwer Academic Publishers, 1988, pp. 113-41.
13. L. Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo p." *Applications of Fibonacci Numbers*, Vol. 3. Ed. G. E. Bergum, A. N. Philippou, and A. F. Horadam. Dordrecht, Holland: Kluwer Academic Publishers, 1990, pp. 311-24.
14. L. Somer, H. Niederreiter, * A. Schinzel. "Maximal Frequencies of Elements in Second-Order Recurrences Over a Finite Field." To appear.

*****