COMPLETE AND REDUCED RESIDUE SYSTEMS OF SECOND-ORDER RECURRENCES MODULO p

Hua-Chieh Li
Department of Mathematics, National Tsing Hua University,
Hsinchu, Taiwan 30043, Republic of China
(Submitted August 1998-Final Revision June 1999)

1. INTRODUCTION

Fix a prime p. We say that a set S forms a complete residue system modulo p if, for all i such that $0 \le i \le p-1$, there exists $s \in S$ such that $s \equiv i \pmod{p}$. We say that a set S forms a reduced residue system modulo p if, for all i such that $1 \le i \le p-1$, there exists $s \in S$ such that $s \equiv i$ (mod p). In [9], Shah showed that, if p is a prime and $p \equiv 1, 9 \pmod{10}$, then the Fibonacci sequence does not form a complete residue system modulo p. For $p > 7$, Bruckner [2] proved this result for the remaining case. Thus, if p is a prime and $p > 7$, then the Fibonacci sequence $\{F_n\}$ has an incomplete system of residues modulo p. Somer [11] generalized these results by considering all linear recurrence sequences with parameters $(a, 1)$, i.e., linear recurrences of the form

$$u_n = au_{n-1} + u_{n-2}.$$

He proved that, if $p > 7$ and $p \not\equiv 1$ or $9 \pmod{20}$, then all recurrence sequences with parameters $(a, 1)$, for which $p \nmid a^2+4$, have an incomplete system of residues modulo p. For the remaining primes, this result has been proved by Schinzel in [8].

In this paper we obtain a unified theory of the structure of recurrence sequences by examining the ratios of recurrence sequences. We can apply our method to prove that, if $p > 7$, then all recurrence sequences with parameters $(a, 1)$, for which $p \nmid a^2+4$, have an incomplete system of residues modulo p. To explain our idea more clearly, we include our proof here. However, our idea is totally different from Schinzel's. Finally, we apply our method to determine for which primes p a second-order recurrence sequence forms a reduced residue system modulo p. Our main result is that, if $p > 17$ and a^2+4 is not a quadratic residue modulo p, then all the recurrence sequences with parameters $(a, 1)$ do not form a reduced residue system modulo p.

2. PRELIMINARIES AND CONVENTIONAL NOTATIONS

Given $a, b \in \mathbb{Z}$, we consider all the second-order linear recurrence sequences $\{u_n\}$ in $\mathbb{Z}$ satisfying $u_n = au_{n-1} + bu_{n-2}$. However, in this paper we exclude the case $u_n = 0$ for all $n \in \mathbb{Z}$. We also exclude the case in which $b \equiv 0 \pmod{p}$ since, in this case, $\{u_n\}$ is not purely periodic modulo p. We call the sequence $\{u_n\}$ a second-order recurrence sequence with parameters (a, b). In particu-lar, the sequence with $u_0 = 0$ and $u_1 = 1$ is called the generalized Fibonacci sequence and we denote it by $\{f_n\}$. The sequence with $u_0 = 2$ and $u_1 = a$ is called the generalized Lucas sequence and we denote it by $\{l_n\}$.

Definition: Let $\{u_n\}$ be a second-order linear recurrence sequence. Consider $r_n = (u_n, u_{n+1})$ as an element in the projective space $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. We call r_n the n^{th} ratio of $\{u_n\}$ modulo p and we call the sequence $\{r_n\}$ the ratio sequence of $\{u_n\}$ modulo p.

We say that two sequences $\{u_n\}$ and $\{u'_n\}$ which both satisfy the same recurrence relation are equivalent modulo p if there is $c \not\equiv 0 \pmod{p}$ and an integer s such that $u_{n+s} \equiv cu'_s \pmod{p}$ for all n. Let $\{r_n\}$ and $\{r'_n\}$ be the ratio sequences of $\{u_n\}$ and $\{u'_n\}$ modulo p, respectively. Then $\{u_n\}$ and $\{u'_n\}$ are equivalent modulo p if and only if there exist integers s and t such that $r_s = r'_t$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$.

Since $\{u_n\}$ is periodic modulo p, the ratio sequence $\{r_n\}$ of $\{u_n\}$ modulo p is also periodic. The least positive integer z such that $r_0 = r_z$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ is called the rank of $\{u_n\}$ modulo p. We remark that the rank of apparition of $\{f_n\}$ modulo p (i.e., the smallest positive integer z such that $f_z \equiv 0 \pmod{p}$), by our definition, equals the rank of $\{f_n\}$ modulo p.

For convenience, we introduce some notation:

(1) (β/p) denotes the Legendre symbol; i.e., for $p \nmid \beta$, $(\beta/p) = 1$ if $y^2 \equiv \beta \pmod{p}$ is solvable and $(\beta/p) = -1$ if $y^2 \equiv \beta \pmod{p}$ is not solvable.

(2) For an integer $m \not\equiv 0 \pmod{p}$, we denote m^{-1} to be the solution of $mx \equiv 1 \pmod{p}$.

(3) We denote the least positive integer t such that $d^t \equiv 1 \pmod{p}$ by $\text{ord}_p(d)$.

Given a sequence $\{u_n\}$, there exists an $r \in \mathbb{Z}$ such that $\{u_n\}$ modulo p is equivalent to the sequence $\{u'_n\}$ modulo p with $u'_0 = 1$ and $u'_1 = r$. Therefore, without loss of generality, we only consider the sequence with $u_0 = 1$ and $u_1 = r$.

The following lemmas are not new. However, for some of the lemmas, we include proofs because these ideas will be used for the proof of our main theorems.

Lemma 2.1: Let $\{u_n\}$ be the recurrence sequence with parameters (a, b) and $u_0 = 1$, $u_1 = r$. Then the rank of $\{u_n\}$ modulo p equals the rank of $\{f_n\}$ modulo p if $r^2 - ar - b \not\equiv 0 \pmod{p}$.

Proof: Suppose the the rank of $\{u_n\}$ modulo p is t and the rank of $\{f_n\}$ modulo p is z. Since $u_n = bf_{n-1} + rf_n$, we have that $u_{z+1} \equiv rf_{z+1} \equiv ru_z \pmod{p}$ because $f_z \equiv 0 \pmod{p}$ and $bf_{z-1} \equiv f_{z+1} \pmod{p}$. This says that $(u_z, u_{z+1}) = (u_0, u_1)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ and hence $t \mid z$. On the other hand, we have that $bf_t + rf_{t+1} \equiv r(bf_{t-1} + rf_t) \pmod{p}$ by the assumption that $u_{t+1} \equiv ru_t \pmod{p}$. Substituting $f_{t+1} = af_t + bf_{t-1}$, we have that $(r^2 - ar - b)f_t \equiv 0 \pmod{p}$. Therefore, $p \nmid r^2 - ar - b$ implies that $f_t \equiv 0 \pmod{p}$. This says that $z \mid t$. □

Lemma 2.2: Let p be an odd prime and let z be the rank of the generalized Fibonacci sequence with parameters (a, b) modulo p. Let $D = a^2 + 4b$. Then

(i) $z \mid p+1$ if $(D/p) = -1$,

(ii) $z = p$ if $p \mid D$,

(iii) $z \mid p-1$ if $(D/p) = 1$.

Proof: ***(i)*** Suppose that $(D/p) = -1$. Then $x^2 - ax - b \equiv 0 \pmod{p}$ has no solution. Thus, by Lemma 2.1, every recurrence sequence with parameters (a, b) has the same rank modulo p. Let t be the number of distinct equivalence classes of recurrence sequences of parameters (a, b) modulo p. Further, let $\{\{u_{i,n}\} \mid 1 \le i \le t\}$ be a representative of these equivalence classes and let $\{\{r_{i,n}\} \mid 1 \le i \le t\}$ be their ratio sequences in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, respectively. By definition, we then have $r_{i,s} \ne r_{i,\lambda}$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ for all $1 \le s \ne \lambda \le z$ and, if $i \ne j$, $\{r_{i,n}\}$ and $\{r_{j,n}\}$ are disjoint. Since, for any $r \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, $(u_0, u_1) = r$ gives a sequence $\{u_n\}$, we have $\{r_{1,1}, \dots, r_{1,z}\} \cup \dots \cup \{r_{t,1}, \dots, r_{t,z}\} = \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. It follows that $tz = p+1$ because the number of elements in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ is $p+1$.

(ii) For $p \mid D$, $x^2 - ax - b \equiv 0 \pmod p$ has a double root. By Lemma 2.1, the number of ratios that give the same rank as the generalized Fibonacci sequence does is $p+1-1 = p$. Our claim follows by a similar argument as in (i) above.

(iii) For $(D/p) = 1$, there exist two distinct solutions to $x^2 - ax - b \equiv 0 \pmod p$. Our claim follows by a similar argument as in (i) above. □

Remark: From the proof above, we have that the number of distinct equivalence classes of recurrence sequences with parameters (a, b) modulo p is $(p+1)/z$ (resp. $2 + (p-1)/z$), if $(D/p) = -1$ (resp. $(D/p) = 1$).

Lemma 2.3: Let z be the rank of the generalized Fibonacci sequence with parameters (a, b) modulo p and let $D = a^2 + 4b$. Suppose that p is an odd prime such that $p \nmid D$. Then $(-b/p) = 1$ if and only if $z \mid \frac{p-(D/p)}{2}$.

Proof: For the proof, please see Lehmer [5]. □

Lemma 2.4: Let $\{f_n\}$ be the generalized Fibonacci sequence with parameters (a, b) and let z be the rank and k be the period of $\{f_n\}$ modulo p, respectively. Let $z = 2^\nu z'$ and $\mathrm{ord}_p(-b) = 2^\mu h$, where z' and h are odd integers.

(i) If $\nu \neq \mu$, then $k = 2\,\mathrm{lcm}[z, \mathrm{ord}_p(-b)]$.

(ii) If $\nu = \mu > 0$, then $k = \mathrm{lcm}[z, \mathrm{ord}_p(-b)]$.

Proof: For the proof, please see Wyler [13]. □

In the following, we concentrate on recurrence sequences with parameters $(a, 1)$.

Lemma 2.5: Let $\{u_n\}$ and $\{u'_n\}$ be two recurrence sequences with parameters $(a, 1)$. Then $u_r u'_s + u_{r+1} u'_{s+1} = u_{r+1} u'_{s-1} + r_{r+2} u'_s$.

Proof: By the recurrence formula, we have that

$$u_{r+1}u'_{s-1} + u_{r+2}u'_s = u_{r+1}(u'_{s+1} - au'_s) + (au_{r+1} + u_r)u'_s = u_{r+1}u'_{s+1} + u_r u'_s. \ \square$$

Lemma 2.6: Let z be the rank of apparition of the generalized Fibonacci sequence modulo p.

(i) $f_i f_{z-i-1} + f_{i+1} f_{z-i} \equiv 0 \pmod p$.

(ii) $f_{\lambda z - t} \equiv \begin{cases} f_{\lambda z + t} \pmod p & \text{if } t \text{ is odd,} \\ -f_{\lambda z + t} \pmod p & \text{if } t \text{ is even.} \end{cases}$

(iii) If z is even, then $f_{z/2-t} \equiv \begin{cases} -f_{z/2+t} \pmod p & \text{if } t \text{ is odd,} \\ f_{z/2+t} \pmod p & \text{if } t \text{ is even.} \end{cases}$

Proof: ***(i)*** Since $1f_{z-2} + af_{z-1} = f_z \equiv 0 \pmod p$ and $f_1 = 1$, $f_2 = a$ by Lemma 2.5, we have that $f_2 f_{z-3} + f_3 f_{z-2} \equiv 0 \pmod p$. By induction, our claim follows.

(ii) Since $f_{\lambda z} \equiv 0 \pmod p$, we have that $f_{\lambda z} f_{\lambda z-1} + f_{\lambda z+1} f_{\lambda z} \equiv 0 \pmod p$. It follows from Lemma 2.5 that $f_{\lambda z+1} f_{\lambda z-2} + f_{\lambda z+2} f_{\lambda z-1} \equiv 0 \pmod p$. We have that $f_{\lambda z-2} \equiv -f_{\lambda z+2} \pmod p$ because $f_{\lambda z-1} \equiv f_{\lambda z+1} \pmod p$. By induction, our claim follows.

(iii) Substitute $i = z/2$ in (i). We have $f_{z/2}f_{z/2-1} + f_{z/2+1}f_{z/2} \equiv 0 \pmod p$. Since $f_{z/2} \not\equiv 0 \pmod p$, it follows that $f_{z/2-1} \equiv -f_{z/2+1} \pmod p$. By induction, our claim follows. □

Since $f_{z+1} \equiv f_{z+1}f_1 \pmod p$ and $f_z \equiv f_{z+1}f_0 \pmod p$, it follows that $f_{n+z} \equiv f_{z+1}f_n \pmod p$ for all n. Suppose that $\{u_n\}$ is a recurrence sequence with parameters $(a, 1)$. Then, as $u_n = u_0 f_{n-1} + u_1 f_n$, we also have $u_{n+z} \equiv f_{z+1}u_n \pmod p$ for all n and, hence, $u_{n+\lambda z} \equiv f_{z+1}^{\lambda}u_n \pmod p$.

Lemma 2.7: Let z be the rank of apparition of the generalized Fibonacci sequence modulo p. Then

(i) $l_{i-1}l_{z-i} + l_i l_{z-i+1} \equiv 0 \pmod p$,

(ii) $l_{\lambda z-t} \equiv \begin{cases} -l_{\lambda z+t} \pmod p & \text{if } t \text{ is odd,} \\ l_{\lambda z+t} \pmod p & \text{if } t \text{ is even.} \end{cases}$

Proof: ***(i)*** Since z is the rank of $\{f_n\}$ modulo p, by the argument above it follows that $(l_z, l_{z+1}) = (l_0, l_1) = (2, a)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. By the recurrence relation, we have that $(l_{z-1}, l_z) = (-a, 2)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. Therefore, we have that $l_0 l_{z-1} + l_1 l_z \equiv 0 \pmod p$. By Lemma 2.5, it follows that $l_1 l_{z-2} + l_2 l_{z-1} \equiv 0 \pmod p$. By induction, our claim follows.

(ii) Since $l_{\lambda z-1} \equiv -l_{\lambda z+1} \pmod p$, we have that $l_{\lambda z}l_{\lambda z-1} + l_{\lambda z+1}l_{\lambda z} \equiv 0 \pmod p$. By Lemma 2.5 it follows that $l_{\lambda z+1}l_{\lambda z-2} + l_{\lambda z+2}l_{\lambda z-1} \equiv 0 \pmod p$. Therefore, $l_{\lambda z-2} \equiv l_{\lambda z+2} \pmod p$. By induction, our claim follows. □

3. COMPLETE RESIDUE SYSTEMS OF SECOND-ORDER RECURRENCES MODULO p

Somer [11] proved that, if $p > 7$, $p \nmid a^2+4$, and $p \not\equiv 1$ or $9 \pmod{20}$, then all recurrence sequences with parameters $(a, 1)$ have an incomplete system of residues modulo p. In Theorem 3.3 we will improve Somer's results to all primes $p > 7$ by substantially extending the methods used in Somer's paper. As remarked earlier, Schinzel [8] proved this result by a different method.

We remark that, if $u_i \equiv 0 \pmod p$ for some i, then the recurrence sequence $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p. Therefore, we only have to consider the sequence that is equivalent to the generalized Fibonacci sequence modulo p. Hence, we reduce our problem to considering whether or not $\{f_n\}$ forms a complete residue system modulo p.

First, we consider the case where $p \nmid a^2+4$ and $x^2 - ax - 1 \equiv 0 \pmod p$ is solvable. In this case, it follows by Lemmas 2.2, 2.3, and 2.4 that the period of $\{f_n\}$ divides $p-1$. Thus, the number of distinct residues of $\{f_n\}$ modulo p is less than p and we conclude that $\{f_n\}$ does not form a complete residue system modulo p.

Now we consider the case where $x^2 - ax - 1 \equiv 0 \pmod p$ is not solvable.

Lemma 3.1: Suppose that $x^2 - ax - 1 \equiv 0 \pmod p$ is not solvable. Let z be the rank of apparition of the generalized Fibonacci sequence modulo p. Consider all recurrence sequences with parameters $(a, 1)$ modulo p. Fix an integer e with $1 \le e < z$. Then, given an integer λ, up to the equivalence relation, there exists a unique $\{u_n\}$ and there exists a unique integer i depending on $\{u_n\}$ with $1 \le i \le z$ such that $u_{i+e} \equiv \lambda u_i \pmod p$.

Proof: Suppose $(u_i, u_{i+1}) = (1, r)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. Then we see by induction that $(u_i, u_{i+e}) = (1, rf_e + f_{e-1})$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. Since $f_e \not\equiv 0 \pmod p$, for $1 \le e < z$, there exists a unique r modulo p

such that $rf_e + f_{e-1} \equiv \lambda \pmod{p}$. For the ratio $(1, r) \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, this gives a unique equivalence class of recurrence sequences modulo p. Let $\{u_n\}$ be a representative of such a class. Since there is no solution for $x^2 - ax - 1 \equiv 0 \pmod{p}$, the rank of $\{u_n\}$ modulo p is equal to z. Therefore, there exists a unique i with $1 \le i \le z$ such that $(u_i, u_{i+1}) = (1, r)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. □

Example: We are particularly interested in the case $\lambda \equiv \pm 1 \pmod{p}$. Consider the recurrence sequences satisfying $u_n = 3u_{n-1} + u_{n-2}$ modulo $p = 7$. We have the generalized Fibonacci sequence

$$\{f_n\}_0^\infty \equiv \{0, 1, 3, 3, 5, 4, 3, 6, 0, 6, 4, 4, 2, 3, 4, 1, 0, \dots\} \pmod{7}.$$

Since $z = 8 = p+1$, every recurrence sequence with parameters $(3, 1)$ is equivalent to $\{f_n\}$ modulo 7. For $e = 3$, we have $f_3 \equiv f_{3+3}$ and $f_2 \equiv -f_{2+3} \pmod{7}$. For $e = 5$, we have $f_5 \equiv f_{5+5}$ and $f_6 \equiv -f_{6+5} \pmod{7}$.

Since Somer has treated the case $p \equiv 3 \pmod{4}$ completely, in the following we only consider the case $p \equiv 1 \pmod{4}$.

For the case $p \equiv 1 \pmod{4}$, by Lemma 2.3, we have that $z \mid (p+1)/2$; hence, by Lemma 2.4, $k = 4z$. Thus, $k \ge p$ occurs only if $z = (p+1)/2$; hence, we have to consider only the case $z = (p+1)/2$. In this case, by the Remark following Lemma 2.2, there are exactly two distinct equivalence classes of recurrence sequences with parameters $(a, 1)$ modulo p. One is equivalent to $\{f_n\}$ modulo p and the other is equivalent to $\{l_n\}$ because of the following.

Lemma 3.2: Let $p \equiv 1 \pmod{4}$ be a prime such that $x^2 - ax - 1 \equiv 0 \pmod{p}$ is not solvable.

(i) The generalized Lucas sequence with parameters $(a, 1)$ is not equivalent to the generalized Fibonacci sequence with parameters $(a, 1)$ modulo p.

(ii) Let z be the rank of $\{f_n\}$ modulo p. Then, for every $t, \lambda \in \mathbb{Z}$, $l_t l_{z-t+\lambda} \equiv (-1)^\lambda l_{t-\lambda} l_{z-t} \pmod{p}$.

Proof: ***(i)*** For $\{f_n\}$, we have $f_n^2 - f_{n-1}f_{n+1} = (-1)^{n-1}$. Suppose that $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p. Then there exist r and j such that $u_n \equiv rf_{n+j} \pmod{p}$ for all n. Thus, $u_n^2 - u_{n-1}u_{n+1} \equiv (-1)^{n+j-1}r^2 \pmod{p}$; hence, it is a quadratic residue modulo p for all n because -1 is a quadratic residue modulo p. On the other hand, $l_n^2 - l_{n-1}l_{n+1} = (-1)^n(a^2+4)$ which, by assumption, is not a quadratic residue modulo p. Our first claim follows.

(ii) Since $\{l_n\}$ is not equivalent to $\{f_n\}$ modulo p, it follows that $l_n \not\equiv 0 \pmod{p}$ for all n. By Lemma 2.7(i), we have that $l_t l_{t-1}^{-1} \equiv -l_{z-t} l_{z-t+1}^{-1}$, $l_{t-1} l_{t-2}^{-1} \equiv -l_{z-t+1} l_{z-t+2}^{-1}, \dots \pmod{p}$. Multiplying on both sides, our proof is complete. □

From the proof above we know that, if $z = (p+1)/2$, then $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p if and only if $u_n^2 - u_{n-1}u_{n+1}$ is a quadratic residue modulo p for all n.

By Lemma 2.6(ii), for each t with $1 \le t \le k = 2(p+1)$, we have that $f_t \equiv \pm f_i \pmod{p}$ for some i, where $1 \le i \le z = (p+1)/2$. Thus, if we can find one pair (i, j), where $1 \le i,\ j \le z-1$, such that $f_i \equiv \pm f_j \pmod{p}$, then the number of distinct residues of $\{f_n\}$ modulo p is less than or equal to $2(z-2)+1 = p-2$ since $f_0 \equiv f_z \equiv 0 \pmod{p}$; hence, $\{f_n\}$ does not form a complete residue system modulo p. We only have to claim that there exists an odd integer e such that $1 \le e < (p+1)/2$ and $f_i \equiv \pm f_{i+e} \pmod{p}$ for some i such that $1 \le i \le z-1$. This claim is sufficient because in this case, if $i+e > z$, then by Lemma 2.6(ii), we have that $f_i \equiv \pm f_{2z-(i+e)} \pmod{p}$ and $1 \le 2z - (i+e) < z$. (Notice that $2z - (i+e) - i$ is also odd.) Now, for a fixed odd integer e, consider the sequence $\{u_n\}$ such that $u_n = f_n - f_{n+e}$. Since e is odd, it follows by the Binet formulas that

$$u_n^2 - u_{n-1}u_{n+1} = (-1)^n(f_{e+1}+f_{e-1}) = (-1)^n l_e.$$

Since $p \equiv 1 \pmod 4$, it follows that there exists i with $1 \le i \le z-1$ such that $f_i \equiv f_{i+e} \pmod p$ if and only if $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p if and only if l_e is a quadratic residue modulo p. Similarly, using the Binet formulas to show that, if $u'_n = f_n + f_{n+e}$, then $(u'_n)^2 - u'_{n-1}u'_{n+1} = (-1)^{n-1}l_e$, we find that there exists j such that $1 \le j \le z-1$ and such that $f_j \equiv -f_{j+e} \pmod p$ if and only if l_e is a quadratic residue modulo p. We remark that l_z is a quadratic residue modulo p since, for $e=z$, $u_0 = f_0 - f_z \equiv 0 \pmod p$.

Theorem 3.3: Let $\{f_n\}$ be the generalized Fibonacci sequence with parameters $(a, 1)$ and let p be a prime such that $p \equiv 1 \pmod 4$ and $(D/p) = -1$, where $D = a^2+4$. Then, for $p>5$, $\{f_n\}$ does not form a complete residue system modulo p.

Proof: Assume that l_e is not a quadratic residue modulo p for all odd integers e such that $1 \le e < z$. We shall get a contradiction.

First, we consider the case $p \equiv 5 \pmod 8$. By substituting $i=(z-1)/2$ in Lemma 2.6(i) and $i=(z+1)/2$ in Lemma 2.7(i), we have that $l_{(z+1)/2}l_{(z-1)/2}^{-1}$ and $f_{(z+1)/2}f_{(z-1)/2}^{-1}$ are solutions to $x^2 \equiv -1 \pmod p$; hence, neither is a quadratic residue modulo p. Note that $l_0 = 2$ is not a quadratic residue modulo p, either. By assumption, $l_1 = a$ is not a quadratic residue modulo p. By Lemma 2.7(i), $l_1 l_0^{-1} \equiv -l_{z-1}l_z^{-1} \pmod p$; hence, l_{z-1} is a quadratic residue modulo p. By the assumption $(l_{z-2}/p) = -1$, we have that $(l_2/p) = 1$ because $l_2 l_1^{-1} \equiv -l_{z-2}l_{z-1}^{-1} \pmod p$. By induction, we have that $(l_i/p) = -1$ for odd i, but $(l_j/p) = 1$ for even j, where $1 \le i,\ j \le z-1$. This means that $l_t l_{t-1}^{-1}$ is not a quadratic residue modulo p for every t such that $2 \le t \le z-1$. Note that every element of $\{l_t l_{t-1}^{-1} \mid 2 \le t \le z-1\}$ is in a distinct residue class modulo p and that there are $z-2 = (p-3)/2$ of them. Because $\{l_n\}$ and $\{f_n\}$ are not equivalent modulo p, $\{l_t l_{t-1}^{-1} \mid 2 \le t \le z-1\}$ and $\{f_t f_{t-1}^{-1} \mid 2 \le t \le z-1\}$ are disjoint modulo p. It follows that among $\{f_t f_{t-1}^{-1} \mid 2 \le t \le z-1\}$ there is only one which is not a quadratic residue modulo p. But we know that neither $f_{(z+1)/2}f_{(z-1)/2}^{-1}$ nor $f_2 f_1^{-1} = a = l_1$ is a quadratic residue modulo p. We get a contradiction because, by the assumption, $p>5$, $(z+1)/2 = (p+3)/4 > 2$.

For the case $p \equiv 1 \pmod 8$, $l_{(z+1)/2}l_{(z-1)/2}^{-1}$ and $f_{(z+1)/2}f_{(z-1)/2}^{-1}$ are roots of $x^2 \equiv -1 \pmod p$; hence, both are quadratic residues modulo p. Note that $l_0 = 2$ is also a quadratic residue modulo p. By the same reasoning as above, we have that $(l_i/p) = -1$ for every integer i such that $1 \le i \le z-1$; hence, $l_t l_{t-1}^{-1}$ is a quadratic residue modulo p for every t such that $2 \le t \le z-1$. Therefore, among $\{f_t f_{t-1}^{-1} \mid 2 \le t \le z-1\}$, $f_{(z+1)/2}f_{(z-1)/2}^{-1}$ is the only quadratic residue modulo p. However, since $f_2 = a = l_1$ is not a quadratic residue modulo p, it follows that $f_4 = f_2 l_2$ is a quadratic residue modulo p. Hence, one of $f_3 f_2^{-1}$ or $f_4 f_3^{-1}$ is a quadratic residue modulo p. We get a contradiction because, by the assumption, $p \ge 17$, $(z+1)/2 = (p+3)/4 > 4$. □

4. REDUCED RESIDUE SYSTEMS OF SECOND-ORDER RECURRENCES MODULO p

From the previous section, we conclude that, if $p>7$ and $p \nmid a^2+4$, then every recurrence sequence $\{u_n\}$ with parameters $(a, 1)$ does not form a complete residue system modulo p.

It would be interesting to know whether or not the recurrence sequence $\{u_n\}$ forms a reduced residue system modulo p.

For the prime p such that $p \mid a^2+4$, since $z=p$, there are exactly two distinct equivalence classes modulo p. One is the equivalence class of $\{f_n\}$ modulo p and the other is the equivalence class of $\{v_n\}$ which satisfies $v_0=1$ and $v_1=\alpha$, where α is the double root of $x^2-ax-1\equiv 0$ (mod p). We already know, by [3], [11], and [12], that $\{f_n\}$ forms a complete residue system modulo p. Moreover, $\{v_n\}$ also forms a reduced residue system modulo p if and only if α is a primitive root modulo p, since $v_n \equiv \alpha^n \pmod{p}$.

Definition: Let α be a root of $x^2-ax-1\equiv 0 \pmod{p}$. We call α a generalized Fibonacci primitive root with parameters $(a, 1)$ modulo p if α is a primitive root modulo p. For the case $a=1$, we call it a Fibonacci primitive root modulo p.

Brison [1], using Hermite's criterion for a permutation polynomial over a finite field (see [6]), proved that, for $p\geq 7$, a recurrence sequence $\{u_n\}$ with parameters $(1, 1)$ has the property that $\{u_1, u_2, \ldots, u_{p-1}\}$ is a reduced residue system modulo p if and only if $\{u_n\}$ is equivalent to the sequence $\{v_n\}$ modulo p, where $v_0=1$ and v_1 is a Fibonacci primitive root modulo p. Brison's method can be applied directly to recurrence sequences with parameters $(a, 1)$. Therefore, we have the following lemma.

Lemma 4.1: Let $p\geq 7$ be a prime. Then a recurrence sequence $\{u_n\}$ with parameters $(a, 1)$ has the property that $\{u_1, u_2, \ldots, u_{p-1}\}$ is a reduced residue system modulo p if and only if $u_2u_1^{-1}$ modulo p is a generalized Fibonacci primitive root with parameters $(a, 1)$ modulo p.

For a prime $p\geq 7$ such that a^2+4 is a quadratic residue modulo p, the period of every recurrence sequence with parameters $(a, 1)$ modulo p divides $p-1$. Therefore, we rephrase Lemma 4.1 as follows.

Proposition 4.2: Let $p\geq 7$ be a prime such that a^2+4 is a quadratic residue modulo p. Then a recurrence sequence $\{u_n\}$ with parameters $(a, 1)$ forms a reduced residue system modulo p if and only if $u_2u_1^{-1}$ modulo p is a generalized Fibonacci primitive root with parameters $(a, 1)$ modulo p.

Fibonacci primitive roots and related topics have an extensive literature. Here, we refer to Shanks [10] and Phong [7].

Lemma 4.1 does not answer our question for primes p such that a^2+4 is not a quadratic residue modulo p, because in this case the period of the recurrence sequence with parameters $(a, 1)$ modulo p may be greater than $p-1$. We have the following example.

Example: Consider the Lucas sequence $\{L_n\}$ (i.e., $L_0=2$, $L_1=1$, and $L_n=L_{n-1}+L_{n-2}$) modulo 13 and 17. We have that

$$\{L_n\}_{n=0}^{7} \equiv \{2, 1, 3, 4, 7, 11, 5, 3\} \pmod{13},$$
$$\{L_n\}_{n=14}^{21} \equiv \{11, 12, 10, 9, 6, 2, 8, 10\} \pmod{13},$$

and

$$\{L_n\}_{n=0}^{9} \equiv \{2, 1, 3, 4, 7, 11, 1, 12, 13, 8\} \pmod{17},$$
$$\{L_n\}_{n=18}^{27} \equiv \{15, 16, 14, 13, 10, 6, 16, 5, 4, 9\} \pmod{17}.$$

Therefore, the Lucas sequence forms a reduced residue system modulo 13 and 17.

We now claim that, for a prime $p>17$ such that a^2+4 is not a quadratic residue modulo p, every recurrence sequence with parameters $(a, 1)$ does not form a reduced residue system modulo p.

Let $\{u_n\}$ be a recurrence sequence with parameters $(a, 1)$. Since $u_n = u_0 f_{n-1} + u_1 f_n$, we have that the period of $\{u_n\}$ modulo p divides the period of $\{f_n\}$ modulo p. Therefore, as before, we only have to consider the cases where the rank of the generalized Fibonacci sequence modulo p is $(p+1)/2$ or $p+1$. If the rank is $p+1$, then, since every sequence is equivalent to $\{f_n\}$ modulo p, it follows that none of the recurrence sequences with parameters $(a, 1)$ forms a reduced residue system modulo p. For the case in which the rank is $(p+1)/2$, by Theorem 3.3, $\{f_n\}$ does not form a complete residue system modulo p. Therefore, we only have to consider the generalized Lucas sequence $\{l_n\}$ modulo p. By Lemma 2.7(ii), for every t with $1 \le t \le k = 2(p+1)$, we have that $l_t \equiv \pm l_i$ for some i, where $0 \le i \le z = (p+1)/2$. Thus, if we can find three distinct pairs (i, j) such that $0 \le i < j \le (p+1)/2$ and $l_i \equiv \pm l_j \pmod p$, then the number of distinct residues of $\{l_n\}$ modulo p is less than or equal to $2(z+1-3) = p-3$; hence, $\{l_n\}$ does not form a reduced residue system modulo p.

For a fixed odd integer e, consider the sequence $\{v_n\}$ such that $v_n = l_n - l_{n+e}$. Since e is odd, we see by the Binet formulas that $v_n^2 - v_{n-1}v_{n+1} = (-1)^{n-1}(a^2+4)l_e$. Since $z = (p+1)/2$, by Lemma 2.3, $p \equiv 1 \pmod 4$. Because a^2+4 is not a quadratic residue modulo p, it follows that there exists $0 \le i \le (p+1)/2$ such that $l_i \equiv l_{i+e} \pmod p$ if and only if $\{v_n\}$ is equivalent to $\{f_n\}$ modulo p if and only if l_e is not a quadratic residue modulo p. Similarly, by using the Binet formulas to show that, if $v'_n = l_n + l_{n+e}$, then $(v'_n)^2 - v'_{n-1}v'_{n+1} = (-1)^n(a^2+4)l_e$, we have that there exists j such that $0 \le j \le z$ and such that $l_j \equiv -l_{j+e} \pmod p$ if and only if l_e is not a quadratic residue modulo p. If there exist three distinct odd integers e such that $0 < e < z$ and l_e is not a quadratic residue modulo p, then, by the routine argument given in the last section, we can find three distinct pairs (i, j) such that $0 \le i < j \le z$ and $l_i \equiv \pm l_j \pmod p$.

Suppose that there are at most two odd integers e such that $0 < e < z$ and l_e is not a quadratic residue modulo p. Then, for p large enough, we claim this leads to a contradiction.

First, we consider the case $p \equiv 1 \pmod 8$. Recall that $z = (p+1)/2$ and l_z must be a quadratic residue modulo p. Since $l_0 = 2$ in this case, we have $(l_0/p) = (l_z/p) = 1$; hence, $(l_1/p) = (l_{z-1}/p)$ by Lemma 2.7(i). Again, by Lemma 2.7(i) and by induction, it follows that $(l_i/p) = (l_{z-1}/p)$ for all $0 \le i \le (z+1)/2$. Note that i is odd if and only if $z-i$ is even. By assumption, there are at most two odd integers e such that $0 < e < z$ and $(l_e/p) = -1$; hence, there are also at most two even integers e such that $0 < e < z$ and $(l_e/p) = -1$. Therefore, among $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$ modulo p, there are at most eight quadratic nonresidues modulo p. Hence, there are at least $(p+1)/2 - 8$ nonzero quadratic residues modulo p in $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$. Since $\{f_i f_{i-1}^{-1} \mid 1 < i < z\}$ and $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$ modulo p form a reduced residue system modulo p, we get a contradiction if we find eight nonzero quadratic residues modulo p among $\{f_i f_{i-1}^{-1} \mid 1 < i < z\}$. Let $s = (z+1)/2$. By Lemma 2.6(i), we have that $f_{s+i} f_{s+i-1}^{-1} \equiv -f_{s-i-1} f_{s-i}^{-1} \pmod p$. Therefore, for s large enough, if we can prove that there exist four integers i with $1 < i < s = (p+3)/4$ such that $f_i f_{i-1}^{-1}$ is a nonzero quadratic residue modulo p, then our claim follows. Recall that $f_{2n} = l_n f_n$. Suppose that e is odd and $(l_e/p) = 1$. Then we have $(f_e/p) = (f_{2e}/p)$ and, since e is odd, it follows that there exists i with $e < i \le 2e$ such that $(f_i/p) = (f_{i-1}/p)$. Thus, $f_i f_{i-1}^{-1}$ is a quadratic residue modulo p. Hence, our strategy is finding s large enough so that we can find four positive odd integers $e(i)$ with $2e(i) < e(i+1)$ for $1 \le i \le 3$ and $2e(4) < s$ such that $(l_{e(i)}/p) = 1$ for all $1 \le i \le 4$. Since, by assumption, we have at most two odd integers e such that $(l_e/p) = -1$, the worst case is that $(l_1/p) = (l_3/p) = -1$. In this case, we can choose $e(1) = 5$, $e(2) = 11$, $e(3) = 23$, and $e(4) = 47$. Therefore, for $s > 94$ (i.e., $p > 373$), we get a contradiction.

Next we consider the case $p \equiv 5 \pmod 8$. Since $l_0 = 2$ in this case, we have that $(l_0/p) = -(l_z/p) = -1$; hence, $(l_1/p) = -(l_{z-1}/p)$ by Lemma 2.7(i). Again, by Lemma 2.7(i) and by induction, it follows that $(l_i/p) = -(l_{z-i}/p)$ for all $0 \le i \le (z+1)/2$. By assumption, there are at most two odd integers e such that $0 < e < z$ and $(l_e/p) = -1$; hence, there are at most two positive even integers e such that $0 < e < z$ and $(l_e/p) = 1$. Thus, among $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$ modulo p, there are at most eight quadratic residues modulo p, so there are at least $(p+1)/2 - 8$ quadratic nonresidues modulo p in $\{l_i l_{i-1}^{-1} \mid 1 \le i \le z\}$. Therefore, by the same argument as above for s large enough, if we can prove that there exist four integers i with $1 < i < s = (p+3)/4$ such that $f_i f_{i-1}^{-1}$ is a quadratic nonresidue modulo p, then our claim follows. Suppose that e is even and $(l_e/p) = -1$. Then we have $(f_e/p) = -(f_{2e}/p)$, and it follows that there exists an integer i with $e < i \le 2e$ such that $((f_i/p) = -(f_{i-1}/p)$. Thus, $f_i f_{i-1}^{-1}$ is a quadratic nonresidue modulo p. Hence, our strategy is finding s large enough so that we are able to discover four positive even integers $e(i)$ with $2e(i) \le e(i+1)$ for $1 \le i \le 3$ and $2e(4) < s$ such that $(l_{e(i)}/p) = -1$ for all $1 \le i \le 4$. The worst case is that $(l_2/p) = (l_4/p) = 1$. In this case, we can choose $e(1) = 6$, $e(2) = 12$, $e(3) = 24$, and $e(4) = 48$. Therefore, for $s > 96$ (i.e., $p > 381$), we get a contradiction.

We remark that, by more detailed investigation, the argument can be narrowed down to the case $s > 13$ (i.e., $p > 49$). However, in order to avoid this complication, we omit the proof here. For the cases $p = 29$, $p = 37$, and $p = 41$, by direct computation, we have that the generalized Lucas sequence with parameters $(a, 1)$ does not form a reduced residue system modulo p. Thus, we have the following theorem.

Theorem 4.3: Let p be a prime such that $a^2 + 4$ is not a quadratic residue modulo p. Then, for $p > 17$, every recurrence sequence $\{u_n\}$ with parameters $(a, 1)$ does not form a reduced residue system modulo p.

In conclusion, we remark that in [11] Somer mentions that, for a more general recurrence sequence (i.e., a recurrence with parameters (a, b), where $b \ne 1$) our results are not always true. The following proposition tells us that, given any prime p, there exists a generalized Fibonacci sequence that forms a complete residue system modulo p.

Proposition 4.4: Suppose that either $p = 2$ or that p is an odd prime, $-b$ is a primitive root modulo p, and $a^2 + 4b$ is not a quadratic residue modulo p. Then the generalized Fibonacci sequence $\{f_n\}$ with parameters (a, b) forms a complete residue system modulo p. Furthermore, every recurrence sequence with parameters (a, b) which is not equivalent to $\{f_n\}$ forms a reduced residue system modulo p.

Proof: The proposition is true by inspection for $p = 2$. Assume $p > 2$. Let z and k be the rank and period of $\{f_n\}$ modulo p, respectively. Since $a^2 + 4b$ is not a quadratic residue modulo p, then $z \mid p+1$ by Lemma 2.2. Furthermore, since $-b$ is not a quadratic residue modulo p, then $z \nmid (p+1)/2$ by Lemma 2.3. Suppose that $p \equiv 1 \pmod 4$. Then $z \equiv 2 \pmod 4$ and, by Theorem

2.4, it follows that $k = 2\gcd[z, p-1] = z(p-1)$. Suppose that $p \equiv 3 \pmod 4$. Then $z \equiv 0$ (mod 4) and, by Theorem 2.4, it follows that $k = 2\gcd[z, p-1] = z(p-1)$. This shows that f_{z+1} is a primitive root modulo p in both cases. Since, for every recurrence sequence $\{u_n\}$ with parameters (a, b), $u_{\lambda z+1} \equiv f_{z+1}^{\lambda} u_1 \pmod p$, our proof is complete. □

Remark: Regarding the statement of Proposition 4.4, we note that, for any odd prime p, one can always find residues a and b modulo p such that $-b$ is a primitive root modulo p and $a^2 + 4b$ is a quadratic nonresidue modulo p. It was proved in [4] that, for a fixed residue b modulo p, one can always find a residue a such that $a^2 + 4b$ is a quadratic nonresidue modulo p.

ACKNOWLEDGMENT

The author would like to express his appreciation to the anonymous referee for making valuable suggestions and helpful comments that improved the presentation of this paper.

REFERENCES

1. O. J. Brison. "Complete Fibonacci Sequences in Finite Fields." *The Fibonacci Quarterly* **30.4** (1992):295-304.
2. G. Bruckner. "Fibonacci Sequence Modulo a Prime $p \equiv 3$ (mod 4)." *The Fibonacci Quarterly* **8.3** (1970):217-20.
3. R. T. Bumby. "A Distribution Property for Linear Recurrence of the Second Order." *Proc. Amer. Math. Soc.* **50** (1975):101-06.
4. G. Kowol. "On Strong Dickson Pseudoprimes." *Appl. Algebra Engrg. Comm. Comput.* **3** (1992):129-38.
5. D. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. of Math.* **31** (1930):419-48.
6. R. Lidl & H. Niederreiter. *Introduction to Finite Fields and Their Applications.* Cambridge: Cambridge University Press, 1991.
7. B. M. Phong. "Lucas Primitive Roots." *The Fibonacci Quarterly* **29.1** (1991):66-71.
8. A. Schinzel. "Special Lucas Sequences, Including the Fibonacci Sequence, Modulo a Prime." In *A Tribute to Paul Erdös*, pp. 349-57. Ed. A. Baker et al. Cambridge: Cambridge University Press, 1990.
9. A. P. Shah. "Fibonacci Sequence Modulo *m*." *The Fibonacci Quarterly* **6** (1968):139-41.
10. D. Shanks. *Solved and Unsolved Problems in Number Theory.* 2nd ed. New York: Chelsea, 1978.
11. L. Somer. "Primes Having an Incomplete System of Residues for a Class of Second-Order Recurrences." In *Applications of Fibonacci Numbers* **2:**113-41. Ed. A. N. Philippou et al. Dordrecht: Kluwer, 1988.
12. W. A. Webb & C. T. Long. "Distribution Modulo p^h of the General Linear Second-Order Recurrence." *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.*(8), **58.2** (1975):92-100.
13. O. Wyler. "On Second Order Recurrences. *Amer. Math. Monthly* **72** (1965):500-06.

AMS Classification Numbers: 11B39, 11A07, 11B50

❖❖❖