ON SECOND-ORDER LINEAR RECURRENCE SEQUENCES: WALL AND WYLER REVISITED

Hua-Chieh Li
Dept. of Mathematics, National Tsing Hua University, Hsin Chu, 300, Taiwan, R.O.C.
(Submitted March 1998-Final Revision April 1999)

1. INTRODUCTION

Sequences of integers satisfying linear recurrence relations have been studied extensively since the time of Lucas [5], notable contributions being made by Carmichael [2], Lehmer [4], Ward [11], and more recently by many others. In this paper we obtain a unified theory of the structure of recurrence sequences by examining the ratios of recurrence sequences that satisfy the same recurrence relation. Results of previous authors usually derived from many complicated identities. Evidently, our method is simple and more conceptual.

The method of using ratios modulo p or over a finite ring has been used in several papers including [1], [3], [6], and [7] among several others. Many known results due to Lucas [5], Lehmer [4], Vinson [9], Wall [10], and Wyler [13] can be derived easily from the well-known method of utilizing ratios. However, our point of view is really different from that of previous authors, so that we obtain our main result (Theorem 3.6(iii)), which improves on a result of Wyler [13], and we also get new information (Corollary 4.3) concerning Wall's question [10].

2. PRELIMINARIES AND CONVENTIONAL NOTATIONS

Given a and b in the ring $\mathcal{R}$ with b a unit, we consider all the second-order linear recurrence sequences $\{u_n\}$ in $\mathcal{R}$ 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 call the sequence $\{u_n\}$ a second-order recurrence sequence with parameters (a, b).

Our idea comes from the following observation: Let $\{u_n\}$ and $\{u'_n\}$ be a pair of sequences in $\mathcal{R}$ that satisfy the same recurrence relation defined above. Suppose that there exists a unit c in $\mathcal{R}$ such that $u_t = cu'_{t+s}$ and $u_{t+1} = cu'_{t+s+1}$ for some integers t and s. Then, since $b \in \mathcal{R}^*$, by the recurrence formula, we have that $u_n = cu'_{n+s}$ for all $n \in \mathbb{Z}$. Recall that the two elements (x_0, x_1) and (y_0, y_1) in the projective space $\mathbb{P}^1(\mathcal{R})$ are the same if $x_0 = cy_0$ and $x_1 = cy_1$ for some $c \in \mathcal{R}^*$. Hence, if we consider (u_n, u_{n+1}) as in the projective space $\mathbb{P}^1(\mathcal{R})$, then $(u_t, u_{t+1}) = (u'_{t+s}, u'_{t+s+1})$ in $\mathbb{P}^1(\mathcal{R})$ for some t implies $(u_n, u_{n+1}) = (u'_{n+s}, u'_{n+s+1})$ in $\mathbb{P}^1(\mathcal{R})$ for all n. We have the following definition.

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

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

In particular, suppose that $u_t = u_{t+s}$ and $u_{t+1} = u_{t+s+1}$ for some integers t and s. Then we have that $u_n = u_{n+s}$ for all n. In this case, we say that $\{u_n\}$ is periodic and the least positive integer k such that $u_0 = u_k$ and $u_1 = u_{k+1}$ is called the period of $\{u_n\}$. When $\{u_n\}$ is periodic, the ratio sequence $\{r_n\}$ of $\{u_n\}$ is also periodic. The least positive integer z such that $r_0 = r_z$ in $\mathbb{P}^1(\mathcal{R})$ is called the rank of $\{u_n\}$. Suppose that the period of $\{u_n\}$ is k and the rank of $\{u_n\}$ is z. It is clear that $z \mid k$ and $r_i \neq r_j$ in $\mathbb{P}^1(\mathcal{R})$ for all $1 \leq i \neq j \leq z$.

We remark that, if $\mathcal{R}$ is a finite ring, then the linear recurrence sequence $\{u_n\}$ is periodic.

3. RECURRENCE SEQUENCE MODULO p

In this section, we will extend our method to treat general second-order linear recurrence sequences. Results in Lucas [5], Lehmer [4], and Wyler [13] can be derived easily using our method.

Fix a and $b \in \mathbb{Z}$. We consider second-order recurrence sequences of parameters (a, b). Thus, we consider the sequences of integers $\{u_n\}_{n=0}^{\infty}$ defined by $u_n = au_{n-1} + bu_{n-2}$ for all integers $n \geq 2$, where u_0 and u_1 are given integers. In the case in which $u_0 = 0$ and $u_1 = 1$, the sequence $\{u_n\}_{n=0}^{\infty}$ is called the *generalized Fibonacci sequence* and we denote its terms by $f_0, f_1, \ldots$.

Fix a prime number p. We consider the recurrence sequence of parameters (a, b) modulo p. Suppose that $p \mid b$. Then it is easy to see that $u_n \equiv a^{n-1}u_1 \pmod{p}$. Therefore, for the remainder of this section, we always assume that $p \nmid b$ and, hence, $\{u_n\}$ is periodic modulo p.

The positive integer z is called the *rank of apparition* of the generalized Fibonacci sequence modulo p if it is the smallest positive integer such that $f_z \equiv 0 \pmod{p}$. Let $r_i = (f_i, f_{i+1})$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ be the i^{th} ratio of $\{f_n\}$ modulo p. Since $r_0 = (0, 1) = r_z$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ and z is the least positive integer such that $r_z = (0, 1)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, it is clear that the rank of apparition of the generalized Fibonacci sequence modulo p is equal to the rank of the generalized Fibonacci sequence modulo p.

Given a sequence $\{u_n\}$, there exists $r \in \mathbb{Z}$ 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 $u_1 = r$.

Lemma 3.1 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^i equals the rank of $\{f_n\}$ modulo p^i if $p \nmid r^2 - ar - b$.

Proof: Suppose that the rank of $\{u_n\}$ modulo p^i is t and the rank of $\{f_n\}$ modulo p^i is z. Set $u'_n = bf_{n-1} + rf_n$. We have that $u'_n \equiv au'_{n-1} + bu'_{n-2} \pmod{p^i}$ and $u'_0 \equiv 1$ and $u'_1 \equiv r \pmod{p^i}$. Thus, $u'_n \equiv u_n \pmod{p^i}$ for all n. Hence, $u_{z+1} \equiv rf_{z+1} \equiv ru_z \pmod{p^i}$ because $f_z \equiv 0 \pmod{p^i}$ and $bf_{z-1} \equiv f_{z+1} \pmod{p^i}$. This says that $(u_z, u_{z+1}) = (u_0, u_1)$ in $\mathbb{P}^1(\mathbb{Z}/p^i\mathbb{Z})$ and, hence, $t \mid z$. On the other hand, we have that $bf_t + rf_{t+1} \equiv r(bf_{t-1} + rf_t) \pmod{p^i}$, by the assumption that $u_{t+1} \equiv ru_t \pmod{p^i}$. Substituting $f_{t+1} = af_t + bf_{t-1}$, we have that $(r^2 - ar - b)f_t \equiv 0 \pmod{p^i}$. Therefore, $(r^2 - ar - b, p) = 1$ implies that $f_t \equiv 0 \pmod{p^i}$. This says that $z \mid t$. □

Remark: Suppose that $r^2 - ar - b \equiv 0 \pmod{p}$ and $\{u_n\}$ is the sequence with parameters (a, b) and $u_0 = 1$, $u_1 = r$. Then we can easily obtain $u_n \equiv r^n u_0 \pmod{p}$. Hence, the rank of $\{u_n\}$ modulo p is 1.

Proposition 3.2 (Lucas): Let z be the rank of the generalized Fibonacci sequence with parameters (a, b) modulo p. Let $D = a^2 + 4b$ and denote $(/)$ to be the Legendre symbol. Then

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

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

(iii) $z = p$, if $p \mid D$.

Proof: (i) Suppose that $(D/p) = -1$. Then $x^2 - ax - b \equiv 0 \pmod{p}$ has no solution. Thus, by Lemma 3.1, every recurrence sequence with parameters (a, b) has the same rank modulo p. Let t be the number of distinct equivalence classes of recurrence sequence of parameters (a, b) modulo p. Let $\{\{u_{i,n}\} \mid 1 \le i \le t\}$ be a representative of these equivalence classes and $\{\{r_{i,n}\} \mid 1 \le i \le t\}$ be their ratio sequences in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. By definition, we have that $r_{i,s} \ne r_{i,t}$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ for all $1 \le s \ne t \le z$ 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 that $\{r_{1,1}, \ldots, r_{1,z}\} \cup \cdots \cup \{r_{t,1}, \ldots, r_{t,z}\} = \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. It follows that $zt = p+1$ because the number of elements in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ is $p+1$.

(ii) For $(D/p) = 1$, there exist two distinct solutions to $x^2 - ax - b \equiv 0 \pmod{p}$. By the Remark following Lemma 3.1, these two solutions give us sequences of rank 1. Consider all the distinct equivalence classes of sequences that have the same rank as the Fibonacci sequence modulo p. As in the above argument, their ratio sequences form disjoint subsets of equal numbers of elements of $^1(\mathbb{Z}/p\mathbb{Z})$. Since the number of these ratios is $p+1-2$, our claim follows.

(iii) Since, for p/D, there exists exactly one solution to $x^2 - ax - b \equiv 0 \pmod{p}$, by the above argument, our claim follows. □

Remark: From the proof of Proposition 3.2, the number of distinct equivalence classes of recurrence sequences with parameters (a, b) that have the same rank z as the generalized Fibonacci sequence modulo p is $(p+1)/z$ (resp. $(p-1)/z, 1$) if $(D/p) = -1$ (resp. $(D/p) = 1, p \mid D$).

Lemma 3.3: Let $\{u_n\}$ and $\{u'_n\}$ be two recurrence sequences with parameters (a, b). Then

$$bu_r u'_s + u_{r+1}u'_{s+1} = bu_{r+1}u'_{s-1} + u_{r+2}u'_s.$$

Proof: By the recurrence formula, we have that

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

Let $r = (a, b)$ and $r' = (a', b')$ be two elements in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ with a, a', b, and $b' \not\equiv 0 \pmod{p}$. Then we define $r \cdot r' = (aa', bb')$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. Let $\{r_n\}$ be the ratio sequence of the generalized Fibonacci sequence modulo p and let z be the rank of the generalized Fibonacci sequence modulo p. Since $bf_{z-2} + af_{z-1} = f_z \equiv 0 \pmod{p}$ and $f_1 = 1, f_2 = a$, we have that $bf_i f_{z-i-1} + f_{i+1}f_{z-i} \equiv 0 \pmod{p}$ by Lemma 3.3 and by induction. This says that $r_i \cdot r_{z-i-1} = (1, -b)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ for $1 \le i \le z-2$. Because $r_1 \cdot r_2 \cdot \cdots \cdot r_{z-2} = (f_1, f_{z-1})$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, we have the following Lemma.

Lemma 3.4: Let $\{f_n\}$ be the generalized Fibonacci sequence with parameters (a, b) and let z be the rank of $\{f_n\}$ modulo p.

(i) If z is even, then $f_{z-1} \equiv (-b)^{(z-2)/2} \pmod{p}$.

(ii) If z is odd, then $f_{z-1} \equiv r(-b)^{(z-3)/2} \pmod{p}$, where $r^2 \equiv -b \pmod{p}$.

We remark that in Lemma 3.4(ii), $r \equiv f_{(z+1)/2} / f_{(z-1)/2} \pmod{p}$.

Since $f_{z+1} \equiv af_z + bf_{z-1} \equiv bf_{z-1}f_1 \pmod{p}$ and $f_z \equiv 0 \equiv bf_{z-1}f_0 \pmod{p}$, it follows that $f_{n+z} \equiv bf_{z-1}f_n \pmod{p}$ for all n and, hence, $f_{n+\lambda z} \equiv (bf_{z-1})^{\lambda} f_n \pmod{p}$. Suppose that $\{u_n\}$ is a recurrence sequence with parameters (a, b). Then, since $u_n = bu_0 f_{n-1} + u_1 f_n$, we also have that $u_{n+z} \equiv bf_{z-1}u_n \pmod{p}$ for all n. Furthermore, suppose that $\{u_n\}$ modulo p is not equivalent to $\{f_n\}$ modulo p and suppose that $\{r_n'\}$ is the ratio sequence of $\{u_n\}$ modulo p. Since $u_n \not\equiv 0 \pmod{p}$ (otherwise $\{u_n\}$ is equivalent to $\{f_n\}$), it follows that $r_1' \cdot r_2' \cdot \cdots \cdot r_z' = (u_1, u_{z+1})$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ and, by the above argument, $(u_1, u_{z+1}) = (1, bf_{z-1})$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$.

Now we consider the product of all the ratios of nonequivalent sequences modulo p with the exception of (f_{z-1}, f_z) and (f_z, f_{z+1}). By Proposition 3.2, we have the following:

(i) If $x^2 - ax - b \equiv 0 \pmod{p}$ is not solvable, then

$$(1, b^{-1}(bf_{z-1})^{(p+1)/z}) = (1, (p-1)!) = (1, -1) \text{ in } \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z}).$$

Hence, $(bf_{z-1})^{(p+1)/z} \equiv -b \pmod{p}$.

(ii) If $x^2 - ax - b \equiv 0 \pmod{p}$ is solvable with a double root γ, then

$$(1, f_{p-1}) \cdot (1, \gamma) = (1, (p-1)!) = (1, -1) \text{ in } \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z}).$$

Notice that $\gamma^2 \equiv -b \pmod{p}$.

(iii) If $x^2 - ax - b \equiv 0 \pmod{p}$ is solvable with two distinct solutions α and β, then

$$(1, b^{-1}(bf_{z-1})^{(p-1)/z}) \cdot (1, \alpha) \cdot (1, \beta) = (1, (p-1)!) = (1, -1) \text{ in } \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z}).$$

Since $\alpha\beta \equiv -b \pmod{p}$, it follows that $(bf_{z-1})^{(p-1)/z} \equiv 1 \pmod{p}$.

Notice that in (ii), since $z = p$ is odd, by Lemma 3.4, $f_{p-1} \equiv (-b)^{(p-3)/2} r \pmod{p}$, where $r \equiv f_{(z+1)/2} / f_{(z-1)/2} \pmod{p}$ and $r^2 \equiv -b \pmod{p}$. We have that $r \equiv -\gamma$ or $r \equiv \gamma \pmod{p}$. Since $-1 \equiv f_{p-1}\gamma \equiv r^{p-2}\gamma \pmod{p}$, it follows that $\gamma \equiv -r \pmod{p}$. Thus, $-f_{(p+1)/2} / f_{(p-1)/2}$ is the double root to $x^2 - ax - b \equiv 0 \pmod{p}$.

Using a similar argument, by considering (i) and (iii), we can improve the results in Proposition 3.2.

Proposition 3.5 (Lehmer): Let z be the rank of the generalized Fibonacci sequence with parametrs (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 $z \left| \frac{p-(D/p)}{2} \right.$.

Proof: If z is odd, then, by Lemma 3.4(ii), we have that $(-b/p) = 1$. Since $p - (D/p)$ is even, we have that $2z \mid p - (D/p)$. Suppose that z is even. Then, by (i) and (iii) above, and by Lemma 3.4, we have that

$$(-1)^{\frac{p-(D/p)}{z}} (-b)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Our proof is complete because $(-b/p) \equiv (-b)^{(p-1)/2} \pmod{p}$. □

From Lemma 3.4, we realize that the relation between the period and the rank of $\{f_n\}$ modulo p depends on the order of $-b$ modulo p. Denote $\mathrm{ord}_p(d)$ to be the least positive integer x such that $d^x \equiv 1 \pmod{p}$. We begin with the following easy observation. For $n \in \mathbb{N}$, we have

$$\operatorname{ord}_p(d^n) = \frac{\operatorname{ord}_p(d)}{\gcd(n, \operatorname{ord}_p(d))}.$$

It is also easy to check that

$$\operatorname{ord}_p(-d) = \begin{cases} \operatorname{ord}_p(d), & \text{if } \operatorname{ord}_p(d) \equiv 0 \pmod 4, \\ \frac{1}{2}\operatorname{ord}_p(d), & \text{if } \operatorname{ord}_p(d) \equiv 2 \pmod 4, \\ 2\operatorname{ord}_p(d), & \text{if } \operatorname{ord}_p(d) \equiv 1 \pmod 2. \end{cases}$$

Furthermore, suppose that $x^2 \equiv d \pmod p$ is solvable and suppose that λ is one of its solutions. Then

$$\operatorname{ord}_p(\lambda) = \begin{cases} 2\operatorname{ord}_p(d), & \text{if } \operatorname{ord}_p(d) \equiv 0 \pmod 2, \\ 2\operatorname{ord}_p(d) \text{ or } \operatorname{ord}_p(d), & \text{if } \operatorname{ord}_p(d) \equiv 1 \pmod 2. \end{cases}$$

We remark that, if $(d/p) = 1$ and $\operatorname{ord}_p(d)$ is odd, then the order of one of the roots of $x^2 \equiv d \pmod p$ is odd and the order of another root is even.

Theorem 3.6: 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 $z = 2^v z'$ and $\operatorname{ord}_p(-b) = 2^\mu h$, where z' and h are odd integers.

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

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

(iii) In the case $v = \mu = 0$.

$$k = \begin{cases} 2\operatorname{lcm}[z, \operatorname{ord}_p(-b)], & \text{if } \operatorname{ord}_p(f_{(z+1)/2} / f_{(z-1)/2}) \text{ is odd}, \\ \operatorname{lcm}[z, \operatorname{ord}_p(-b)], & \text{if } \operatorname{ord}_p(f_{(z+1)/2} / f_{(z-1)/2}) \text{ is even}. \end{cases}$$

Proof: First, we consider the case $v > 0$. Since z is even, by Lemma 3.4 and the discussion following Lemma 3.4, we have that $k/z = \operatorname{ord}_p(b(-b)^{(z-2)/2}) = \operatorname{ord}_p(-(-b)^{z/2})$. Suppose $v > \mu$. Then $\operatorname{ord}_p((-b)^{z/2}) = h/\gcd(z', h) \equiv 1 \pmod 2$. Hence, $k/z = 2h/\gcd(z', h)$. Therefore, $k = 2\operatorname{lcm}[z, \operatorname{ord}_p(-b)]$. On the other hand, suppose $\mu = v$. Then $\operatorname{ord}_p((-b)^{z/2}) = 2h/\gcd(z', h) \equiv 2 \pmod 4$. Thus, $k/z = h/\gcd(z', h)$, and hence, $k = \operatorname{lcm}[z, \operatorname{ord}_p(-b)]$. Similarly, suppose $\mu > v$. Then $\operatorname{ord}_p((-b)^{z/2}) = 2^{\mu-v+1}h/\gcd(z', h) \equiv 0 \pmod 4$. Therefore, $k/z = 2^{\mu-v+1}h/\gcd(z', h)$, and hence, $k = 2\operatorname{lcm}[z, \operatorname{ord}_p(-b)]$. Now we consider the case $v = 0$. Since z is odd, we have $k/z = \operatorname{ord}_p(b(-b)^{(z-3)/2}r)$, where $r = f_{(z+1)/2} / f_{(z-1)/2}$ and $r^2 \equiv -b \pmod p$. Hence, $k/z = \operatorname{ord}_p(-r^z)$. Suppose $\mu > v$. Then $\operatorname{ord}_p(r) = 2\operatorname{ord}_p(-b)$; hence, $\operatorname{ord}_p(r^z) = 2\operatorname{ord}_p(-b)/\gcd(z, h) \equiv 0 \pmod 4$. Therefore, $k/z = 2\operatorname{ord}_p(-b)/\gcd(z, h)$; hence, $k = 2\operatorname{lcm}[z, \operatorname{ord}_p(-b)]$. Finally, suppose $\mu = v = 0$. Then either $\operatorname{ord}_p(r) = \operatorname{ord}_p(-b)$ or $\operatorname{ord}_p(r) = 2\operatorname{ord}_p(-b)$. Suppose $\operatorname{ord}_p(r) = \operatorname{ord}_p(-b)$ (that is, $\operatorname{ord}_p(r)$ is odd). Then $\operatorname{ord}_p(r^z) = \operatorname{ord}_p(-b)/\gcd(z, h) \equiv 1 \pmod 2$. Therefore, $k/z = 2\operatorname{ord}_p(-b)/\gcd(z, h)$; hence, $k = 2\operatorname{lcm}[z, \operatorname{ord}_p(-b)]$. On the other hand, suppose $\operatorname{ord}_p(r) = 2\operatorname{ord}_p(-b)$ (that is, $\operatorname{ord}_p(r)$ is even). Then $\operatorname{ord}_p(r^z) = 2\operatorname{ord}_p(-b)/\gcd(z, h) \equiv 2 \pmod 4$. Thus, $k/z = \operatorname{ord}_p(-b)/\gcd(z, h)$ and hence, $k = \operatorname{lcm}[z, \operatorname{ord}_p(-b)]$. □

Remark: Cases (i) and (ii) of Theorem 3.6 above are stated as Wyler's main theorem in [13]. However, our approach is different and Wyler does not settle the case in which both z and $\operatorname{ord}_p(-b)$ are odd (that is, case (iii) of our theorem).

4. RECURRENCE SEQUENCE MODULO p^t

We now treat the case of the generalized Fibonacci sequence modulo p^t for $t \geq 2$.

Let us denote by $z(p^i)$ the rank of $\{f_n\}$ modulo p^i. We begin with an easy observation: If $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p^t, then the number of possible ratios of $\{u_n\}$ modulo p^{t+1} is $z(p^t)$ or $pz(p^t)$. By Lemma 3.1, the rank of such a sequence modulo p^{t+1} equals $z(p^{t+1})$. Therefore, the rank of $z(p^{t+1})$ divides $pz(p^t)$. Since $z(p^t) \mid z(p^{t+1})$, it follows that either $z(p^{t+1}) = z(p^t)$ or $z(p^{t+1}) = pz(p^t)$.

Theorem 4.1: The rank of apparition of the generalized Fibonacci sequence modulo p^t equals the rank of apparition of the generalized Fibonacci sequence modulo p^{t+1} if and only if there exists a sequence which is equivalent to $\{f_n\}$ modulo p^t but is not equivalent to $\{f_n\}$ modulo p^{t+1}.

Proof: $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p^t if and only if $(u_1, u_2) = (f_i, f_{i+1})$ in $\mathbb{P}^1(\mathbb{Z}/p^t\mathbb{Z})$ for some i. On the other hand, by the above argument, $z(p^{t+1}) = z(p^t)$ if and only if there exists $r \in \mathbb{Z}$ such that $(1, r) = (f_i, f_{i+1})$ in $\mathbb{P}^1(\mathbb{Z}/p^t\mathbb{Z})$ for some i but $(1, r) \neq (f_j, f_{j+1})$ in $\mathbb{P}^1(\mathbb{Z}/p^{t+1}\mathbb{Z})$ for all $j \in \mathbb{Z}$. Combining these two statements, our proof is complete. □

We remark that $\{u_n\}$ is equivalent to $\{f_n\}$ modulo p^t if and only if $u_i \equiv 0 \pmod{p^t}$ for some i.

Example: Consider the Fibonacci sequence

$$\{F_n\}_1^\infty \equiv \{1,1,2,3,5,0,5,5,2,7,1,0,1,1,\ldots\} \pmod 8$$

and the Lucas sequence

$$\{L_n\}_1^\infty \equiv \{1,3,4,7,3,2,5,7,4,3,7,2,1,3,\ldots\} \pmod 8.$$

The rank of apparition of the Fibonacci sequence modulo 2, 4, and 8 is 3, 6, and 6, respectively. We have that $\{L_n\}$ is equivalent to $\{F_n\}$ modulo 4 because $L_3 \equiv 0 \pmod 4$ but $\{L_n\}$ is not equivalent to $\{F_n\}$ modulo 8 because $L_n \not\equiv 0 \pmod 8$ for all n.

For every $t \in \mathbb{N}$, we denote $k(p^t)$ to be the period of $\{f_n\}$ modulo p^t. By considering the "Binet form" of $\{f_n\}$, Lehmer [4] proves that, for $p \neq 2$, if $k(p^l) = k(p)$ but $k(p^{l+1}) \neq k(p)$, then $k(p^t) = p^{t-l}k(p)$ for all $t \geq l$. Let $z(p^t)$ denote the rank of apparition of $\{f_n\}$ modulo p^t. By a similar method, we can prove that, for $p \neq 2$, if $z(p^l) = z(p)$ but $z(p^{l+1}) \neq z(p)$, then $z(p^t) = p^{t-l}z(p)$ for all $t \geq l$. We note that this result was also proved by Lucas [5] and by Carmichael [2]. We remark that $z(p^{l+1}) \neq z(p^l)$ implies $k(p^{l+1}) \neq k(p^l)$, but the converse is not always true.

Corollary 4.2: Let $\{f_n\}$ be the generalized Fibonacci sequence with parameters (a, b). Let p be an odd prime and, for every $t \in \mathbb{N}$, denote $z(p^t)$ to be the rank of $\{f_n\}$ modulo p^t. Suppose that

$z(p^l) \neq z(p^{l+1})$. If $\{u_n\}$ is a recurrence sequence with parameters (a, b) such that $u_i \equiv 0 \pmod{p^l}$ for some i, then, for every $t \geq l$, there exists j_t such that $u_{j_t} \equiv 0 \pmod{p^t}$.

Proof: $z(p^l) \neq z(p^{l+1})$ implies $z(p^t) \neq z(p^{t+1})$ for all $t \geq l$. Therefore, according to Theorem 4.1, every sequence that is equivalent to $\{f_n\}$ modulo p^l is also equivalent to $\{f_n\}$ modulo p^t for all $t \geq l$. □

Now we restrict ourselves to considering only the Fibonacci sequence $\{F_n\}$. For every $t \in \mathbb{N}$, we denote $K(p^t)$ to be the period of $\{F_n\}$ modulo p^t. In [10], Wall asked whether $K(p) = K(p^2)$ is always impossible; until this day, it remains an open question. According to Williams [12], $K(p) \neq K(p^2)$ for every odd prime p less than 10^9. Z.-H. Sun and Z.-W. Sun [8] proved that the affirmative answer to Wall's question implies the first case of Fermat's last theorem.

Let $Z(p^t)$ denote the rank of apparition of the Fibonacci sequence modulo p^t for every $t \in \mathbb{N}$. We have that, for $p \neq 2$, $K(p^t) = K(p^{t+1})$ if and only if $Z(p^t) = Z(p^{t+1})$. What makes Theorem 4.1 so interesting is the following Corollary.

Corollary 4.3: Let p be an odd prime and, for every $t \in \mathbb{N}$, denote $K(p^t)$ to be the period of $\{F_n\}$ modulo p^t. Suppose that $K(p^l) \neq K(p^{l+1})$. Let $\{u_n\}$ be a sequence satisfying the same recurrence relation as $\{F_n\}$ such that $u_i \equiv 0 \pmod{p^l}$ for some i. Then, for every $t \geq l$, there exists j_t such that $u_{j_t} \equiv 0 \pmod{p^t}$.

Remark: In particular, let p be an odd prime such that $K(p) \neq K(p^2)$. Suppose that $\{u_n\}$ is a recurrence sequence with parameters $(1, 1)$ and $u_i \equiv 0 \pmod{p}$ for some i. Then Corollary 4.3 implies that, for every positive integer t, there exists j_t such that $u_{j_t} \equiv 0 \pmod{p^t}$. This is true for $p < 10^9$ according to Williams [12].

Unlike the Fibonacci case, we have examples for which $k(p) = k(p^2)$ and $z(p) \neq z(p^2)$.

Example: Let $a = 8$ and $b = -7$. Then $\{f_n\}_{n=0}^{\infty} \equiv \{0,1,3,2,0,1,\ldots\} \pmod 5$ and $\{f_n\}_{n=0}^{\infty} \equiv \{0,1,8, 7,0,1,\ldots\} \pmod{25}$. Consider the sequence $\{u_n\}$ with $u_0 = 5$, and $u_1 = 1$ which satisfies $u_n = 8u_{n-1} - 7u_{n-2}$. We have that $\{u_n\}_{n=0}^{\infty} \equiv \{0,1,3,2,0,1,\ldots\} \pmod 5$ and $\{u_n\}_{n=0}^{\infty} \equiv \{5,1,23,2,5,1,\ldots\} \pmod{25}$.

One might ask for what kind of parameters (a, b) the generalized Fibonacci sequence has $k(p) = k(p^2)$, and whether or not $k(p) = k(p^2)$ for infinitely many primes. From our construction above, we understand that this question is related to: "For a given integer x, does there exist a prime p such that $\mathrm{ord}_p(x) = \mathrm{ord}_{p^2}(x)$?" and "Are there infinitely many primes p such that, for a given integer x, $\mathrm{ord}_p(x) = \mathrm{ord}_{p^2}(x)$?". Of course, we can suppose that $f(x) = x^2 - ax - b$ is irreducible over the integers. Then we have to consider our question over the ring of integers of $\mathbb{Q}[\sqrt{a^2 + 4b}]$. We have not taken up in this paper the question of whether a given recurrence $\{u_n\}$ has zeros modulo a given integer m or not. Ward [11] has shown that $\{u_n\}$ has zeros modulo p for infinitely many primes p. For given parameters (a, b), suppose that we know there are only finitely many primes such that $z(p) = z(p^2)$. Then, by Corollary 4.2, it follows that there exist infinitely many primes p such that $\{u_n\}$ has zeros modulo p^t for every $t \in \mathbb{N}$.

ACKNOWLEDGMENT

The author would like to express his appreciation to the anonymous referee for making valuable suggestions regarding the presentation of this paper.

REFERENCES

1. G. Bruckner. "Fibonacci Sequence Modulo a Prime $p \equiv 3 \pmod 4$." *The Fibonacci Quarterly* **8.3** (1970):217-20.
2. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Ann. of Math.* **15** (1913):30-70.
3. P. Catlin. "On the Divisors of Second-Order Recurrences." *The Fibonacci Quarterly* **12.2** (1974):175-78.
4. D. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. of Math.* **31** (1930):419-48.
5. E. Lucas. "Theorie des fonctions numeriques implement periodiques." *Amer. J. Math.* **1** (1878):184-240, 289-321.
6. L. Somer. "The Fibonacci Ratios F_{k+1} / F_k Modulo p." *The Fibonacci Quarterly* **13.4** (1975): 322-24.
7. 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, A. F. Horadam, & G. E. Bergum. Dordrecht: Kluwer, 1988.
8. Z.-H. Sun & Z.-W. Sun. "Fibonacci Numbers and Fermat's Last Theorem." *Acta Arith.* **60** (1992):371-88.
9. J. Vinson. "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence." *The Fibonacci Quarterly* **1.1** (1963):37-45.
10. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960:525-32.
11. M. Ward. "Prime Divisors of Second-Order Recurrences." *Duke Math. J.* **21** (1954):607-14.
12. H. C. Williams. "A Note on the Fibonacci Quotient $F_{p-\varepsilon} / p$." *Canadian Math. Bull.* **25** (1982):366-70.
13. O. Wyler. "On Second-Order Recurrences." *Amer. Math. Monthly* **72** (1965):500-06.

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

❖❖❖