A NOTE ON A THEOREM OF SCHINZEL

Jukka Pihko
University of Helsinki, Hallituskatu 15 SF-00100 Helsinki, Finland
(Submitted December 1989)

1. Introduction

Consider a sequence defined by the condition

(1.1) $u_0 = 0,\ u_1 = 1,\ u_{n+2} = au_{n+1} + u_n,\ n = 0, 1, 2, \ldots \quad (a \in \mathbb{Z}).$

If $a = 1$, then $u_n = F_n$, that is, we get the sequence of Fibonacci numbers. If p is a fixed prime, we also consider the sequence $\overline{u}_0, \overline{u}_1, \overline{u}_2, \ldots$ defined by the same condition in $\mathbb{F}_p$, the finite field of p elements. Let $k = k(p)$ be the length of the shortest period of the sequence $\overline{u}_0, \overline{u}_1, \overline{u}_2, \ldots$. A Schinzel [1] has proved the following result.

Theorem 1.1 (Schinzel): Let $S = S(p)$ be the set of frequencies with which different residues occur in the sequence $\overline{u}_n$ $[0 \le n < k(p)]$. For $p > 7$, $p \nmid a(a^2 + 4)$ we have

$$S = \{0, 1, 2\} \text{ or } \{0, 1, 2, 3\} \text{ if } k(p) \not\equiv 0 \pmod 4,$$
$$S = \{0, 2, 4\} \text{ if } k(p) \equiv 4 \pmod 8,$$
$$S = \{0, 1, 2\} \text{ or } \{0, 2, 3\} \text{ or } \{0, 1, 2, 4\} \text{ or } \{0, 2, 3, 4\} \text{ if } k(p) \equiv 0 \pmod 8.$$

The purpose of this note is to show how this result can be extended, using the same method, with some minor modifications. Consider the sequence defined by the condition

(1.2) $v_0 = 2,\ v_1 = a,\ v_{n+2} = av_{n+1} + v_n,\ n = 0, 1, 2, \ldots .$

If $a = 1$, then $v_n = L_n$, that is, we get the sequence of Lucas numbers. Consider also the sequence $\overline{v}_0, \overline{v}_1, \overline{v}_2, \ldots$ defined by the same condition in $\mathbb{F}_p$. Let $k' = k'(p)$ be the length of the shortest period of the sequence $\overline{v}_0, \overline{v}_1, \overline{v}_2, \ldots$. We prove that $k' = k$ (Lemma 2.1 below) and get the following result.

Theorem 1.2: Let $S' = S'(p)$ be the set of frequencies with which different residues occur in the sequence v_n $[0 \le n < k(p)]$. For $p > 7$, $p \nmid a(a^2 + 4)$ we have

$$S' = \{0, 1, 2\} \text{ or } \{0, 1, 2, 3\} \text{ if } k(p) \not\equiv 0 \pmod 4,$$
$$S' = \{0, 1, 2\} \text{ or } \{0, 2, 3\} \text{ or } \{0, 1, 2, 4\} \text{ or } \{0, 2, 3, 4\} \text{ if } k(p) \equiv 0 \pmod 4.$$

Moreover,

(1.3) $S' = S$ if $k(p) \not\equiv 4 \pmod 8$.

Corresponding to Schinzel's three corollaries, we deduce from Theorem 1.2 the following corollaries.

Corollary 1.3: If $p > 7$, $p \nmid a^2 + 4$, then at least one residue mod p does not occur in the sequence $\overline{v}_n$.

Corollary 1.4: If $p \ne 5$, $p \nmid a(a^2 + 4)$, then at least one residue mod p occurs exactly twice in the shortest period of the sequence $\overline{v}_n$.

Corollary 1.5: For $a = 1$, $p > 7$,

$$S' = \{0, 1, 2, 3\} \text{ if } k(p) \not\equiv 0 \pmod 4,$$
$$S' = \{0, 1, 2\} \text{ or } \{0, 2, 3\} \text{ or } \{0, 1, 2, 4\} \text{ or } \{0, 2, 3, 4\} \quad \text{if } k(p) \equiv 4 \pmod 8,$$
$$S' = \{0, 1, 2, 4\} \text{ or } \{0, 2, 3, 4\} \text{ if } k(p) \equiv 0 \pmod 8.$$

L. Somer [2] has proved Corollary 1.3 except for the case where $p \equiv 1$ or 9 (mod 20).

2. Some Lemmas

Let $D = a^2 + 4$ and let ξ be a zero of $x^2 - ax - 1$ in the finite field $\mathbb{F}_q$, where $q = p$ if $\left(\frac{D}{p}\right) = 1$ and $q = p^2$ if $\left(\frac{D}{p}\right) = -1$ (we exclude the case $p|D$).

For $\overline{u}_n$ and $\overline{v}_n$ we have the formulas

$$\overline{u}_n = \frac{\xi^n - (-\xi^{-1})^n}{\xi + \xi^{-1}}, \quad \overline{v}_n = \xi^n + (-\xi^{-1})^n. \tag{2.1}$$

Let δ be the least positive exponent such that $\xi^\delta = 1$.

The following seven lemmas correspond to the lemmas in [1].

Lemma 2.1: For $p \nmid 2D$, we have $k'(p) = [\delta, 2] = k(p)$. (Here, the symbol $[\delta, 2]$ means the least common multiple of δ and 2.)

Proof: The second equation above is the content of Lemma 1 in [1]. The first equation follows by exactly analogous considerations using (2.1). □

Lemma 2.2: Let $p \nmid 2D$. The conditions

$$n \equiv m \pmod 2 \text{ and } \overline{v}_n = \overline{v}_m$$

hold if and only if either $n \equiv m \pmod k$ or $n \equiv m \equiv 0 \pmod 2$ and $n + m \equiv 0 \pmod k$ or $k \equiv 0 \pmod 4$, $n \equiv m \equiv 1 \pmod 2$ and $n + m \equiv k/2 \pmod k$.

Proof: We use (2.1) and combine arguments in the proofs of Lemma 2 and Lemma 3 in [1]. □

Lemma 2.3: Let $p \nmid 2D$. The conditions

$$n \equiv m \pmod 2 \text{ and } \overline{v}_n = -\overline{v}_m$$

are equivalent to

$$n \equiv m \equiv 1 \pmod 2 \text{ and } n + m \equiv 0 \pmod k \text{ if } k \equiv 2 \pmod 4,$$

$$n \equiv m + k/2 \pmod 2 \text{ and } \overline{v}_n = \overline{v}_{m+k/2} \text{ if } k \equiv 0 \pmod 4.$$

Proof: We use (2.1) and combine arguments in the proofs of Lemma 2 and Lemma 3 in [1]. □

Lemma 2.4: Let $p \nmid 2D$ and let $0 \le n < k$. We have $\overline{v}_n = 0$ if and only if

$$k \equiv 2 \pmod 4 \text{ and } n = k/2,$$
$$k \equiv 0 \pmod 8 \text{ and } n = k/4 \text{ or } n = 3k/4.$$

Proof: Analogous to the proof of Lemma 4 in [1]. □

Lemma 2.5: Let $p \nmid 2D$. We have

$$k|p - 1 \text{ if } \left(\frac{D}{p}\right) = 1, \quad k|2(p + 1) \text{ if } \left(\frac{D}{p}\right) = -1.$$

Proof: In view of Lemma 2.1, this is exactly the same as Lemma 5 in [1]. □

Lemma 2.6: If $k = 2(p + 1) \equiv 0 \pmod 8$, then for every nonnegative integer e there is an n such that

(2.2) $\quad \overline{v}_{n+e} = \overline{v}_n.$

Proof: If $\overline{u}_e \neq 0$, we use the identity

$$v_n v_{m+e} - v_m v_{n+e} = (-1)^{m+1} D u_e u_{n-m}$$

and find by virtue of Lemma 4 in [1] that the quotients

$$\frac{\overline{v}_{n+e}}{\overline{v}_n} \text{ for } 0 \leq n < \frac{k}{2},\ n \neq \frac{k}{4}$$

are all distinct. Since $k/2 = p + 1$, we have p distinct elements of $\mathbb{F}_p$. One of them must be 1, which gives (2.2).

Suppose now that $\overline{u}_e = 0$. By Lemma 4 in [1], $e \equiv 0 \pmod{k/2}$. It follows from Lemma 2.4 that we can take $n = k/4$. □

Lemma 2.7: Let $p \nmid 2D$. We have

$$\sum_{j=0}^{k/2-1} \overline{v}_{2j}^2 = k, \quad \sum_{j=0}^{k/2-1} \overline{v}_{2j+1}^2 = -k, \quad \sum_{j=0}^{k-1} \overline{v}_j^4 = 6k.$$

Proof: Analogous to the proof of Lemma 7 in [1]. □

We remark that Lemma 2.6 and the last equation in Lemma 2.7 will not be used in this paper.

3. Proof of Theorem 1.2

To prove Theorem 1.2 we shall consider successively the cases $k \not\equiv 4 \pmod 8$ and $k \equiv 4 \pmod 8$. In the first case we prove (1.3).

1. Let $k \not\equiv 4 \pmod 8$. It follows from Lemma 2.4 that 0 occurs in the sequence $\overline{v}_n$ $(0 \leq n < k)$. Thus, the sequence $\overline{v}_n$ $(0 \leq n < k)$ is a non-zero multiple of a translation of the sequence $\overline{u}_n$ $(0 \leq n < k)$. In fact, if t is the least positive integer such that $\overline{v}_n = 0$, then $-t$ is the amount by which the sequence $\overline{u}_n$ $(0 \leq n < k)$ is translated and $\overline{v}_{t+1}$ is the constant multiplier. It then follows immediately that the sequences $\overline{v}_n$ $(0 \leq n < k)$ and $\overline{u}_n$ $(0 \leq n < k)$ have the same frequency pattern of residues appearing in these sequences. (1.3) now follows immediately.

2. Let $k \equiv 4 \pmod 8$. According to Lemma 2.4, 0 does not occur in the sequence $\overline{v}_n$ $(0 \leq n < k)$ so that $0 \in S'$.

According to Lemma 2.2, every element in the sequence $\overline{v}_{2j}$ $(0 \leq 2j < k)$ occurs there exactly twice, except for the elements $\overline{v}_0$ and $\overline{v}_{k/2}$, which occur once. Moreover, $\overline{v}_{k/2} = -\overline{v}_0$ by Lemma 2.3. Similarly, every element in the sequence $\overline{v}_{2j+1} (0 \leq j < k/2)$ occurs there exactly twice, except for the elements $\overline{v}_{k/4}$ and $\overline{v}_{3k/4} = -\overline{v}_{k/4}$, which occur once.

Since $k \equiv 0 \pmod 4$, it follows from Lemma 2.1 that $\delta = k$ and, therefore, $\xi^{k/2} = -1$. Using (2.1), we see that

(3.1) $\quad \overline{v}_{k/4}^2 = \overline{v}_{3k/4}^2 = -4.$

We assume now that $2 \notin S'$. Consider the elements $\overline{v}_{2j} (0 < 2j < k/2)$. These must occur in the sequence $\overline{v}_{2j+1}$ $(0 \leq 2j + 1 < k)$. Since by Lemma 2.3

$$\overline{v}_{2j} = -\overline{v}_{k/2-2j}$$

there are two cases:

I. $\overline{v}_{2j} \neq \pm\overline{v}_{k/4}$ $(0 < 2j < k/2)$,

and

II. $\overline{v}_{2j'} = \overline{v}_{k/4}$ and $\overline{v}_{k/2-2j'} = \overline{v}_{3k/4}$ for some j' $(0 < 2j' < k/2)$.

We shall consider these two cases separately.

Case I: In this case of the two sequences

$$\overline{v}_{2j} \quad (0 \leq 2j < k,\ j \neq 0,\ j \neq k/4)$$

and

$$\overline{v}_{2j+1} \quad (0 \leq 2j+1 < k,\ 2j+1 \neq k/4,\ 2j+1 \neq 3k/4)$$

one is a permutation of the other. Using (3.1), it follows that

$$\sum_{j=0}^{k/2-1} \overline{v}_{2j}^2 - 2(4) = \sum_{j=0}^{k/2-1} \overline{v}_{2j+1}^2 - 2(-4),$$

from which we infer, using Lemma 2.7, that $2k \equiv 16 \pmod{p}$, $k \equiv 8 \pmod{p}$.

It follows from Lemma 2.5 that either

$$k = 2(p+1) \quad \text{or} \quad k \leq p+1.$$

If $k = 2(p+1)$, then $k \equiv 8 \pmod{p}$ implies $3 \equiv 0 \pmod{p}$, which contradicts the assumption $p > 7$. If $k \leq p+1$, then we must have $k = 8$, which contradicts the assumption $k \equiv 4 \pmod{8}$.

Case II: In this case, there are two different elements in the sequence $\overline{v}_{2j+1}$ $(0 \leq 2j+1 < k)$ which occur twice in this sequence and which are not equal to any element $\overline{v}_{2j}$ $(0 < 2j < k/2)$. Since we are assuming that $2 \notin S'$, these elements must appear in the sequence $\overline{v}_{2j}$ $(0 \leq 2j < k)$ and, therefore, they must be $\overline{v}_0$ and $\overline{v}_{k/2} = -\overline{v}_0$. It follows that the sequences $\overline{v}_{2j}$ $(0 \leq 2j < k)$ and $\overline{v}_{2j+1}$ $(0 \leq 2j+1 < k)$ consist of the same elements. Moreover, $\overline{v}_0$ and $\overline{v}_{k/2}$, which occur in the former sequence once, occur in the latter sequence twice and the elements $\overline{v}_{2j'} = \overline{v}_{k/4}$ and $\overline{v}_{k/2-2j'} = \overline{v}_{3k/4}$, occurring in the former sequence twice, occur in the latter sequence once. It follows that

$$\sum_{j=0}^{k/2-1} \overline{v}_{2j}^2 - 2(4) - 4(-4) = \sum_{j=0}^{k/2-1} \overline{v}_{2j+1}^2 - 4(2) - 2(-4),$$

from which we obtain, using Lemma 2.7, that $2k \equiv -16 \pmod{p}$, $k \equiv -8 \pmod{p}$. In a similar manner to that in Case I, we conclude that either $5 \equiv 0 \pmod{p}$, a contradiction, or $k = p - 8 \equiv 1 \pmod{2}$, which contradicts Lemma 2.1.

The assumption $2 \notin S'$ thus leads to a contradiction in every case, so that we have proved that $2 \in S'$.

Now we prove that either $1 \in S'$ or $3 \in S'$ but not both. We must again look at the four elements $\overline{v}_0$, $\overline{v}_{k/2}$, $\overline{v}_{k/4}$, and $\overline{v}_{3k/4}$. It is clear that our assertion is true if we prove that the following four conditions are equivalent:

(3.2) $\quad \exists n \equiv 1 \pmod{2}$ such that $\overline{v}_n = \overline{v}_0$,

(3.3) $\quad \exists n \equiv 1 \pmod{2}$ such that $\overline{v}_n = \overline{v}_{k/2}$,

(3.4) $\quad \exists n \equiv 0 \pmod{2}$ such that $\overline{v}_n = \overline{v}_{k/4}$,

(3.5) $\quad \exists n \equiv 0 \pmod{2}$ such that $\overline{v}_n = \overline{v}_{3k/4}$.

Since $\overline{v}_{k/2} = -\overline{v}_0$ and $\overline{v}_{3k/4} = -\overline{v}_{k/4}$ it follows from Lemma 2.3 that

$$(3.2) \Leftrightarrow (3.3) \quad \text{and} \quad (3.4) \Leftrightarrow (3.5).$$

It remains to be proved that

$$(3.2) \Leftrightarrow (3.4).$$

<u>(3.2) ⇒ (3.4)</u> Suppose that $n \equiv 1 \pmod 2$, $\bar{v}_n = \bar{v}_0$. We prove that

(3.6) $\quad \bar{v}_{n+k/4} = \bar{v}_{k/4}.$

Since $k/4 \equiv 1 \pmod 2$, this will prove (3.4). It follows from (2.1) that

(3.7) $\quad \xi^n - 1 = \xi^{-n} + 1$

and that (3.6) is equivalent to the equation

$$\xi^{n+k/4} + \xi^{-n-k/4} = \xi^{k/4} - \xi^{-k/4},$$

which, using (3.7), can be written as

(3.8) $\quad (\xi^n - 1)(\xi^{k/4} + \xi^{-k/4}) = 0.$

It follows from Lemma 4 in [1] that $\bar{u}_{k/4} = 0$. This, by (2.1), implies that (3.8) holds. Therefore, also (3.6) holds and we have proved the implication (3.2) ⇒ (3.4).

<u>(3.4) ⇒ (3.2)</u> Suppose that $n \equiv 0 \pmod 2$ and $\bar{v}_n = \bar{v}_{k/4}$. We prove that

(3.9) $\quad \bar{v}_{n+3k/4} = \bar{v}_0.$

Using (2.1), the equation (3.9) can be written as

(3.10) $\quad \xi^{n+3k/4} - \xi^{-n-3k/4} = 2.$

We find

$$\begin{aligned}\xi^{n+3k/4} &= (-\xi^{-n} + \xi^{k/4} - \xi^{-k/4})\xi^{3k/4} = -\xi^{-n+3k/4} + \xi^k - \xi^{k/2}\\ &= -\xi^{-n+3k/4} + 1 - (-1),\end{aligned}$$

so that (3.10) will follow if we show that

(3.11) $\quad \xi^{-n+3k/4} + \xi^{-n-3k/4} = \xi^{-n}(\xi^{3k/4} + \xi^{-3k/4}) = 0.$

But

$$(\xi^{3k/4} + \xi^{-3k/4})^2 = (\xi^{k/2})^3 + 2 + (\xi^{-k/2})^3 = (-1)^3 + 2 + (-1)^3 = 0,$$

so that (3.11) follows and the implication (3.4) ⇒ (3.2) is proved.

It has now been proved that the conditions (3.2)-(3.5) are all equivalent.

Since every residue occurs at most twice among $\bar{v}_{2j}$ $(0 \le 2j < k)$ and at most twice among $\bar{v}_{2j+1}$ $(0 < 2j+1 < k)$ it occurs at most four times among $\bar{v}_n$ $(0 \le n < k)$. It follows from what has been proved that, in the case $k \equiv 4 \pmod 8$, we have

$$S' = \{0, 1, 2\} \text{ or } \{0, 2, 3\} \text{ or } \{0, 1, 2, 4\} \text{ or } \{0, 2, 3, 4\}.$$

This completes the proof of Theorem 1.2. □

Proof of Corollary 1.3: For $p \nmid a$, this corollary follows directly from Theorem 1.2. For $p \mid a$, we have $\bar{v}_n = 0$ or 2; hence, $0 \in S'$. □

Proof of Corollary 1.4: If $k \not\equiv 4 \pmod 8$, then $S' = S$ by (1.3) and $2 \in S'$ follows from Schinzel's Corollary 2. Corollary 1.4 clearly holds for $p = 2$ by inspection. If $k \equiv 4 \pmod 8$, then the proof that $2 \in S'$ in the proof of Theorem 1.2 holds if $p > 7$. However, by (3.1), if $k \equiv 4 \pmod 8$, then

$$\bar{v}_{k/4}^2 = \bar{v}_{3k/4}^2 = -4,$$

which implies $p = 2$ or $p \equiv 1 \pmod 4$. Thus, $2 \notin S'$ can hold only if $p = 5$. □

Remark 3.1: Corollary 1.4 is not formulated as generally as the corresponding Corollary 2 in [1]. Example 3.2 shows that $2 \notin S'$ can occur if $p = 5$.

Example 3.2: Take $a = 2$ and $p = 5$, $p \nmid a(a^2 + 4) = 16$. Then $S' = \{0, 3\}$. In fact, the shortest period consists of the residues 2, 2, 1, 4, 4, 2, 3, 3, 4, 1, 1, 3. Note that in this case $k = 2p + 2 = 12 \equiv -8 \pmod{p}$ which was a possibility in Case II.

Proof of Corollary 1.5: This corollary follows from Corollary 3 in [1] and Theorem 1.2. □

We conclude this note by making the following observation. We can look at Corollary 2 in [1] and the corresponding Corollary 1.4 at the same time and calculate the *smallest residue which appears exactly twice in the shortest period*. Keeping the integer a fixed and considering primes $p > 5$, $p \nmid a(a^2 + 4)$ let us denote these residues by $sr_2\bar{u}(p)$ and $sr_2\bar{v}(p)$. It therefore follows from Lemma 4 in [1] and Lemma 2.4 above that we have the following result:

$$sr_2\bar{u}(p) = 0 \Leftrightarrow sr_2\bar{v}(p) = 0 \Leftrightarrow k(p) \equiv 0 \pmod{8}.$$

Acknowledgment

I wish to thank the referee for shortening the proof of Theorem 1.2 and for a better formulation of Corollary 1.4.

References

1. A. Schinzel. "Special Lucas Sequences, Including the Fibonacci Sequence, Modulo a Prime." In *A Tribute to Paul Erdös*. Ed. A. Baker, B. Bollobás, and A. Hajnal. Cambridge: Cambridge University Press, 1990, pp. 349-57.
2. L. Somer. "Primes Having an Incomplete System of Residues for a Class of Second-Order Recurrences." In *Applications of Fibonacci Numbers*. Ed. A. F. Horadam, A. N. Philippou, and G. E. Bergum. Dordrecht: Kluwer Academic Publishers, 1988, pp. 113-41.

*****