DISTRIBUTION OF TWO-TERM RECURRENCE SEQUENCES MOD P^e

Dana Carroll
Department of Mathemetics, Ohio University, Athens, OH 45701

Eliot Jacobson
Department of Mathematics, Ohio University, Athens, OH 45701

Lawrence Somer
Department of Mathematics, Catholic University of America, Washington, D.C. 20064
(*Submitted November 1992*)

INTRODUCTION

In [8], A. Schinzel studied the distribution of the residues of certain two-term recurrence sequences modulo a prime p, and classified the sets of distribution frequencies that occur according to the length of a full period. In the present work, we demonstrate a kind of stability that arises in one case of Schinzel's work, which allows an extension of his classification to prime powers. We conclude by giving some examples that show his results do not extend as naturally in the other cases. Related results concerning distribution questions for recurrence sequences can be found in [1]-[7] and [10]-[13].

DEFINITIONS AND NOTATION

Define the two-term recurrence relation

$$u_0 = 0,\ u_1 = 1,\ u_n = Au_{n-1} + u_{n-2} \text{ for } n > 1,$$

where $A \neq 0$ is a fixed rational integer. Let $p > 7$ be prime, $p \nmid A(A^2+4)$. Let ξ be a real root of $f(x) = x^2 - Ax - 1$ in its splitting field K over $\mathbb{Q}$, and let $\mathcal{R}$ denote the ring of integers in K. Let $\mathcal{P}$ be a prime ideal of $\mathcal{R}$ lying over (p) in $\mathbb{Z}$. By assumption on p, we do not incur any ramification. It will be clear during our discourse that any splitting that may occur is not a problem. Let $0 < e \in \mathbb{Z}$, and let $\delta(p^e)$ denote the order of $\xi + \mathcal{P}^e$ in $\mathcal{R}/\mathcal{P}^e$. Note that since ξ divides 1 in $\mathcal{R}$, $\delta(p^e)$ exists for all e. For notational ease, for $x \in \mathcal{R}$ we denote $x + \mathcal{P}^e$ by $\overline{x}$. Define $k(p^e)$ to be the length of a shortest period of $\overline{u}_n$ and $S(p^e)$ to be the set of residue frequencies within any full period of $\overline{u}_n$. Note that since u_n is a rational integer for all n, studying $u_n \pmod{\mathcal{P}^e}$ is equivalent to studying $u_n \pmod{p^e}$.

We prove the following theorem.

MAIN THEOREM

Let $p > 7$ be prime and $e \geq 1$. If $k(p) \equiv 4 \pmod 8$, then $S(p^e) = \{0, 2, 4\}$.

We need some results from [8] and [16], which are stated here for the reader's convenience.

Ward [16, pp. 619-20]. Let t be the largest integer with $k(p) = k(p^t)$. Then $k(p^e) = pk(p^{e-1})$ for $e > t$.

In fact, Wall [15] conjectured that $k(p) \neq k(p^2)$ for every p in the special case of the Fibonacci sequence, but this remains a difficult and open problem.

Schinzel [8, Theorem 1]. For $p > 7$ prime, and $p \nmid A(A^2+4)$,

(1) if $k(p) \equiv 4 \pmod 8$, then $S(p) = \{0, 2, 4\}$;

(2) if $k(p) \equiv 0 \pmod 8$, then $S(p) = \{0, 1, 2\}$ or $\{0, 2, 3\}$ or $\{0, 1, 2, 4\}$ or $\{0, 2, 3, 4\}$;

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

The proof of the Main Theorem will proceed by induction on e, after some preliminary lemmas.

Lemma 1. The Binet formula

$$u_n = \frac{\xi^n - (-\xi^{-1})^n}{\xi + \xi^{-1}}$$

holds in K, and in $\mathcal{R} / \mathcal{P}^e$, for $e \geq 1$.

Proof: Observe that ξ and $-\xi^{-1}$ are the distinct roots of $f(x)$, hence

$$\begin{aligned}(\xi + \xi^{-1})^2 &= \xi^2 + 2 + \xi^{-2} \\ &= A\xi + 1 + 2 - A\xi^{-1} + 1 \\ &= A(\xi - \xi^{-1}) + 4 \\ &= A^2 + 4,\end{aligned}$$

which is nonzero in K, and hence $\xi + \xi^{-1}$ is a unit in K. The condition that $p \nmid A(A^2+4)$ ensures that $\xi + \xi^{-1}$ is a unit mod $\mathcal{P}^e$. Lemma 1 now follows easily by induction on n. □

For the rest of the paper, we assume additionally that $k(p) \equiv 4 \pmod 8$. Hence, Ward's result gives immediately that $k(p^e) \equiv 4 \pmod 8$ for every $e \geq 1$.

Lemma 2. For every $e \geq 1$, $k(p^e) = \delta(p^e)$.

Proof: Set $k = k(p^e)$ and $\delta = \delta(p^e)$. Since k is even, and $\overline{u}_k = \overline{0}$, $\overline{u}_{k+1} = \overline{1}$, it follows from Lemma 1 that $\overline{\xi}^k - \overline{\xi}^{-k} = \overline{0}$ and $\overline{\xi}^{k+1} + \overline{\xi}^{-k-1} = \overline{\xi} + \overline{\xi}^{-1}$. Thus,

$$\begin{aligned}\overline{\xi}^{k+1} + \overline{\xi}^{k-1} = \overline{\xi} + \overline{\xi}^{-1} &\Rightarrow (\overline{\xi}^k - \overline{1})(\overline{\xi} + \overline{\xi}^{-1}) = \overline{0} \\ &\Rightarrow \overline{\xi}^k = \overline{1}.\end{aligned}$$

Hence $\delta \mid k$.

Since $\delta(p) \mid \delta(p^e)$, it will follow that $\delta(p^e)$ is even if we can show that $\delta(p)$ is even. But this follows directly from [8, Lemma 1] and the fact that $k(p) \equiv 4 \pmod 8$, so that $\overline{u}_\delta = \overline{0}$ and $\overline{u}_{\delta+1} = \overline{1}$, and thus $k \leq \delta$. □

Definition: Let n_{p^e} denote the smallest positive integer n such that $p^e \mid u_n$, called the *rank of apparition of* p^e.

Lemma 3: For every $e \geq 1$, $\overline{u}_n = \overline{0}$ if and only if $n \equiv 0 \left(\mathrm{mod}\ \frac{k(p^e)}{4}\right)$, that is, $n_{p^e} = k(p^e)/4$.

Proof: First note that $\overline{\xi}(\overline{\xi} - \overline{A}) = \overline{1}$, so $\overline{\xi}$ is a unit. Thus,

$$\begin{aligned}\overline{u}_n = \overline{0} &\Leftrightarrow \overline{\xi}^n - (-\overline{\xi}^{-1})^n = \overline{0} \\ &\Leftrightarrow \overline{\xi}^n = (-\overline{\xi}^{-1})^n \\ &\Leftrightarrow \overline{\xi}^{2n} = (-\overline{1})^n.\end{aligned}$$

If n is odd, then since $\delta(p^e) \equiv 4 \pmod 8$, $\overline{\xi}^{2n} = -\overline{1} \Leftrightarrow \overline{\xi}^{4n} = \overline{1} \Leftrightarrow \delta(p^e) = k(p^e) | 4n$.

If n is even, then since $k(p^e)/4$ is odd, $\overline{\xi}^{2n} = \overline{1} \Leftrightarrow \delta(p^e) | 2n \Leftrightarrow k(p^e)/4 | n$. □

Lemma 4: For all n, $h \geq 0$,

$$u_{n+h} - u_n = (\xi^h - 1)u_n + (-\xi^{-1})^n u_h.$$

Proof: By Lemma 1,

$$\begin{aligned}(\xi^h - 1)u_n + (-\xi^{-1})^n u_h &= \frac{1}{\xi + \xi^{-1}}\left((\xi^h - 1)(\xi^n - (-\xi^{-1})^n) + (-\xi^{-1})^n(\xi^h - (-\xi^{-1})^h)\right) \\ &= \frac{1}{\xi + \xi^{-1}}\left(\xi^{n+h} - \xi^n + (-\xi^{-1})^n - (-\xi^{-1})^{n+h}\right) \\ &= u_{n+h} - u_n. \ \square\end{aligned}$$

Lemma 5: Let $A(d; p^e)$ denote the number of times the residue d appears within a full period of $\{u_n\} \pmod{p^e}$. If $k(p^e) \equiv 4 \pmod 8$, then $A(d; p^e)$ is even.

Proof: Denote $k = k(p^e)$. First, if n is even, then by Lemmas 1 and 2,

$$\begin{aligned}\overline{u}_{k/2-n} &= \frac{\xi^{k/2-n} - (-\xi^{-1})^{k/2-n}}{\xi + \xi^{-1}} \\ &= \frac{\xi^{k/2}\xi^{-n} - (-\xi^{-1})^{k/2}(-\xi^{-1})^{-n}}{\xi + \xi^{-1}} \\ &= \frac{-\xi^{-n} + \xi^n}{\xi + \xi^{-1}} \\ &= \overline{u}_n.\end{aligned}$$

Similarly, if n is odd, then $\overline{u}_{k-n} = \overline{u}_n$. Since $k \equiv 4 \pmod 8$, the result follows. □

For the rest of the paper, assume $e > t$, where t is the largest integer with $k(p) = k(p^t)$, and let $k = k(p^{e-1})$. Define the $p \times k$ integer matrix T by setting $T_{ij} \equiv u_{(i-1)k+j-1} \pmod{p^e}$, where $0 \leq T_{ij} < p^e$. Then each row of T is congruent to a full period modulo p^{e-1}, and the rows laid end to end correspond to a full period modulo p^e. We will show that the entries in any column of T are distinct.

Lemma 6: The first column of T has distinct entries.

Proof: Assume that $\overline{u}_{ik} = \overline{u}_{tk}$ for some $0 \le i < t \le p-1$. By Lemma 4,

$$\overline{u}_{tk} - \overline{u}_{ik} = \overline{0} = (\overline{\xi}^{(t-i)k} - 1)\overline{u}_{ik} + (-\overline{\xi}^{-1})^{ik}\overline{u}_{(t-i)k}.$$

Since $\xi^k \equiv 1 \pmod{p^{e-1}}$ by Lemma 2, we have

$$\xi^{(t-i)k} - 1 \in \mathcal{P}^{e-1}. \tag{1}$$

Clearly $u_{ik} \in \mathcal{P}^{e-1}$, therefore, $(\xi^{(t-i)k} - 1)u_{ik} \in \mathcal{P}^{2e-2} \subseteq \mathcal{P}^e$ and, hence, $u_{(t-i)k} \in \mathcal{P}^e$ also. Thus, $n_{p^e} | (t-i)k$. But $n_{p^e} = pn_{p^{e-1}}$ and $k = 4n_{p^{e-1}}$, so $p | 4(t-i)$, a contradiction. □

Lemma 7: Every column of T has distinct entries.

Proof: Assume that $\overline{u}_{ik+j} = \overline{u}_{tk+j}$ for some $0 < j \le k-1$, $0 \le i < t \le p-1$. By Lemma 4,

$$u_{tk+j} - u_{tk} = (\xi^j - 1)u_{tk} + (-\xi^{-1})^{tk}u_j,$$

and

$$u_{ik+j} - u_{ik} = (\xi^j - 1)u_{ik} + (-\xi^{-1})^{ik}u_j.$$

Subtracting these equations, and using the assumption,

$$\overline{u}_{ik} - \overline{u}_{tk} = (\overline{\xi}^j - 1)(\overline{u}_{tk} - \overline{u}_{ik}) + \overline{u}_j\left((-\overline{\xi}^{-1})^{tk} - (-\overline{\xi}^{-1})^{ik}\right)$$

so that

$$\overline{\xi}^j(\overline{u}_{tk} - \overline{u}_{ik}) = -\overline{u}_j\left((-\overline{\xi}^{-1})^{tk} - (-\overline{\xi}^{-1})^{ik}\right).$$

By Lemma 6, $u_{tk} - u_{ik} \in \mathcal{P}^{e-1} \setminus \mathcal{P}^e$ and hence

$$-u_j(-\xi^{-1})^{ik}\left((-\xi^{-1})^{(t-i)k} - 1\right) \in \mathcal{P}^{e-1} \setminus \mathcal{P}^e. \tag{2}$$

By Lemma 1, setting $n = tk + j$ and $m = ik + j$, and noting that $n+m$ is even,

$$\begin{aligned}\overline{0} &= (\overline{u}_n - \overline{u}_m)(\overline{\xi} + \overline{\xi}^{-1}) \\ &= \overline{\xi}^n - (-\overline{\xi}^{-1})^n - \overline{\xi}^m + (-\overline{\xi}^{-1})^m \\ &= \overline{\xi}^m(\overline{\xi}^{n-m} - \overline{1})\left(\overline{1} + (-1)^n(-\overline{\xi}^{-1})^{n+m}\right).\end{aligned}$$

Since p does not divide $t-i$, it follows that $\xi^{n-m} - 1 = \xi^{(t-i)k} - 1 \in \mathcal{P}^{e-1} \setminus \mathcal{P}^e$. Therefore, $1 + (-1)^n(-\xi^{-1})^{n+m} \in \mathcal{P}$ and thus $\xi^{2(n+m)} - 1 \in \mathcal{P}$. Then $k(p) | 2(n+m) = 2(t+i)k + 4j$. Since $k(p) | k$, we get $k(p) | 4j$ and so $p | u_j$. Finally, this gives $u_j \in \mathcal{P}$ and hence $((-\xi^{-1})^{(t-i)k} - 1) \notin \mathcal{P}^{e-1}$ by (2), which contradicts (1). □

PROOF OF MAIN THEOREM

Assume $p > 7$ is a prime with $p \nmid A(A^2+4)$ and $k(p) \equiv 4 \pmod 8$. The case $e = 1$ is just Schinzel's result.

As before, let t be the largest integer such that $k(p) = k(p^t)$. It is easy to see that $\{|u_n|\}$ is a strictly increasing sequence for $n \ge 2$. Since $u_1 = 1$ and $u_2 = A$, it follows that t exists. We now consider the case in which $t > 1$. Let $1 < e \le t$. Let $A(d; p^e)$ be as in Lemma 5. Clearly, $A(d; p^e) \le A(d; p)$. Since $\{0\} \subset S(p)$, it follows that $0 \in S(p^e)$. By Lemma 3, $k(p^e) = 4n_{p^e}$.

Thus, $A(0; p^e) = 4$ and $4 \in S(pe)$. By Lemma 5, $A(d; p^e)$ is even for every residue d. Since $2 \in S(p)$, there is a residue d such that $A(d; p) = 2$. Let u_n be such that $u_n \equiv d \pmod{p}$, and suppose $u_n \equiv d' \pmod{p^e}$. Since $A(d'; p^e)$ is even, $A(d'; p^e) \geq 1$, and $A(d'; p^e) \leq A(d; p) = 2$, we must have $A(d'; p^e) = 2$. Thus, $S(p^e) = \{0, 2, 4\}$

We now proceed by induction on e. Assume the theorem is true for $e-1$, $e \geq t+1$. By Ward's theorem, $k(p^e) \equiv 4 \pmod{8}$.

Let x be any residue modulo p^e appearing in T. Let j be the least positive integer such that $u_j \equiv x \pmod{p^e}$, and let $0 \leq y < p^{e-1}$ satisfy $u_j \equiv y \pmod{p^{e-1}}$. By hypothesis, y occurs either two or four times in any full period modulo p^{e-1}.

Notice any two entries in the same column of T are congruent modulo p^{e-1}, since their subscripts differ by a multiple of $k(p^{e-1})$. Hence, y will occur in either two columns or four columns of T. Since $x = ap^{e-1} + y$ for some $0 \leq a < p$, x must occur once in each of the same columns, and nowhere else, so x will occur in T either two or four times. Thus, $S(p^e) \subseteq \{0, 2, 4\}$. Since there is at least one residue modulo p that does not occur in T, there will also be at least one residue modulo p^e not occurring in T, so $S(p^e) = \{0, 2, 4\}$. □

Remark: It follows by the proof of the Main Theorem that if $e > t$, then $A(d; p^e) = A(d; p^t)$.

Examples: We have shown that in the case $k(p) \equiv 4 \pmod{8}$, Schinzel's result holds for any power of p; that is, $S(p^e) = \{0, 2, 4\}$ for all $e \geq 1$. We give examples here to show that an analogous generalization does not hold in the other cases of Schinzel's result.

First, we consider the case $k \not\equiv 0 \pmod{4}$. There are two subcases to consider:

(1) $S(p) = \{0, 1, 2, 3\}$. If $A = 1$ and $p = 11$, then $S(p^2) = \{0, 1, 2, 3, 11\}$.

(2) $S(p) = \{0, 1, 2\}$. If $A = 4$ and $p = 19$, then $S(p^2) = \{0, 1, 2, 19\}$.

Next, we consider $k \equiv 0 \pmod{8}$. There are four subcases to consider:

(1) $S(p) = \{0, 1, 2, 4\}$. If $A = 1$ and $p = 23$, then $S(p^2) = \{0, 2, 4, 23\}$.

(2) $S(p) = \{0, 1, 2\}$. If $A = 3$ and $p = 11$, then $S(p^2) = \{0, 2, 11\}$.

(3) $S(p) = \{0, 2, 3\}$. If $A = 2$ and $p = 17$, then $S(p^2) = \{0, 2, 19\}$.

(4) $S(p) = \{0, 2, 3, 4\}$. If $A = 2$ and $p = 11$, then $S(p^2) = \{0, 2, 4, 13\}$.

REFERENCES

1. G. Bruckner. "Fibonacci Sequences Modulo a Prime $p \equiv 3 \pmod{4}$." *The Fibonacci Quarterly* **8.3** (1970):217-20.
2. S. A. Burr. "On Moduli for Which the Fibonacci Sequence Contains a Complete System of Residues." *The Fibonacci Quarterly* **9.5** (1971):497-504.
3. E. T. Jacobson. "A Brief Survey on Distribution Questions for Second Order Linear Recurrences." In *Proceedings of the First Meeting of the Canadian Number Theory Association*, pp. 249-54. Ed. Richard A. Mollin. Walter de Gruyter, 1990.
4. E. T. Jacobson. "Distribution of the Fibonacci Numbers Mod 2^k." *The Fibonacci Quarterly* **30.3** (1992):211-15.
5. H. Niederreiter, A. Schinzel, & L. Somer. "Maximal Frequencies of Elements in Second-Order Recurrences over a Finite Field." *Elem. Math.* **46** (1991):139-43.

6. J. Pihko. "A Note on a Theorem of Schinzel." *The Fibonacci Quarterly* **29.4** (1991):333-38.
7. A. P. Shah. "Fibonacci Sequences Modulo *m*." *The Fibonacci Quarterly* **6.2** (1968):139-41.
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, B. Bollobás, & A. Hajnal. Cambridge: Cambridge University Press, 1990.
9. L. Somer. "The Divisibility Properties of Primary Lucas Recurrences with Respect to Primes." *The Fibonacci Quarterly* **18.4** (1980):316-34.
10. L. Somer. "Primes Having an Incomplete System of Residues for a Class of Second-Order Linear Recurrences." In *Applications of Fibonacci Nubmers* **2**:113-41. Ed. A. N. Philippou, A. F. Horadam, & G. E. Bergum. Dordrecht: Kluwer, 1988.
11. L. Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo *p*." In *Applications of Fibonacci Numbers* **3**:311-24. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecht: Kluwer, 1990.
12. L. Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo *p*—II." *The Fibonacci Quarterly* **29.1** (1991):72-78.
13. L. Somer. "Upper Bounds for Frequencies of Elements in Second-Order Recurrences over a Finite Field." In *Applications of Fibonacci Numbers* **5** (to appear).
14. 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.
15. D. D. Wall. "Fibonacci Series Modulo *m*." *Amer. Math. Monthly* **67** (1960):525-32.
16. M. Ward. "The Arithmetical Theory of Linear Recurring Sequences." *Trans. Amer. Math. Soc.* **35** (1933):600-28.

AMS Classification Numbers: 11B50, 11K36

❖❖❖