ON LINEAR RECURRENCES AND DIVISIBILITY BY PRIMES

J. O. SHALLIT and J. P. YAMRON
University of California, Berkeley, CA 94720
(Submitted March 1983)

I. INTRODUCTION

Recently Neumann & Wilson [6] and Shannon & Horadam [8] have discussed the sequence of numbers given by the linear recurrence

$$T_k = T_{k-2} + T_{k-3};\ T_0 = 3,\ T_1 = 0,\ T_2 = 2.$$

This sequence has the following interesting property:

$$\text{If } p \text{ is a prime, then } p|T_p. \tag{1}$$

The sequence $\{T_k\}$ has been discussed several times before; for example, see [1], [2], [3], [4], [5], and [7]. In particular, Perrin [7] asks if the converse to (1) is true, that is:

Does $p|T_p$ imply that p is prime?

Neumann & Wilson call a counterexample to the converse a *pseudoprime*. They did not find any pseudoprimes for the sequence $\{T_k\}$.

Unfortunately, the converse is false; the first example being

$$271441 = 521^2.$$

The only other composite n less than 1000000 for which $n|T_n$ is

$$904631 = 7 \cdot 13 \cdot 9941.$$

These numbers were found using a computer program written in APL and were checked independently by John Hughes using a FORTRAN program.

It can be shown that the sequence $\{T_k\}$ is, essentially, exponential in growth. In particular, for large k we have

$$T_k \sim \alpha^k,$$

where α is the real root of $x^3 - x - 1 = 0$ and $\alpha = 1.32$, approximately.

In [8], Shannon & Horadam remark that the sequence $\{T_k\}$ "is possibly the slowest growing integer sequence for which $p|T_p$ for all primes p." This is clearly false, as simple examples like

$$A_k = k \cdot |\log k|$$

or even

$$A_k = k$$

will show. These examples might be dismissed as trivial. In this note we will show that there exist nontrivial sequences $\{T_k\}$ given by a linear recurrence having the property (1) that have rates of growth like

$$T_k \sim \alpha^k,$$

where $\alpha - 1$ is a positive number arbitrarily close to 0.

II. SLOWLY-GROWING SEQUENCES

Let $n \geqslant 3$ be a positive integer and define

$$f(x) = x^n - x - 1.$$

Let the roots of $f(x) = 0$ be

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

and put

$$T_k = \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k.$$

Then it is easy to see that

$$T_k = T_{k+1-n} + T_{k-n},$$

where the starting values are given by

$$T_0 = n,\ T_1 = 0,\ T_2 = 0,\ \ldots,\ T_{n-2} = 0,\ T_{n-1} = n - 1.$$

By Theorem 2 of [6], the sequence $\{T_k\}$ has the property of (1).

We have the following:

Theorem

Let $f(x) = x^n - x - 1$. Then:

(1) All zeros of f are smaller in magnitude than $3^{1/n}$.

(2) All zeros of f are of multiplicity 1.

(3) f has exactly 1 real zero if n is odd and exactly 2 real zeros if n is even.

(4) f has a real zero α satisfying $2^{1/n} < \alpha < 3^{1/n}$. If n is even, there is in addition a real zero β satisfying $-1 < \beta < 0$.

(5) The positive real zero α is in fact the zero of f largest in magnitude.

Proof:

(1) Let α be the zero of f which is largest in magnitude. Then, for some integer $k \geqslant 0$, we have

$$k^{1/n} \leqslant |\alpha| < (k + 1)^{1/n}.$$

Now $\alpha^n = \alpha + 1$, so

$$|\alpha^n| = |\alpha + 1| \leqslant |\alpha| + 1 < (k + 1)^{1/n} + 1,$$

whereas $k \leqslant |\alpha^n|$. Hence

$$k < (k + 1)^{1/n} + 1$$

and so certainly $k < 3$.

(2) Put $g(x) = nf(x) - xf'(x)$. Now, if there were a repeated zero of f, it would be a zero of f' and hence also a zero of g. But g is linear; in fact,

$$g(x) = (1 - n)x - n.$$

It is easily verified that the zero of g, namely $n/(1 - n)$, is not a zero of f'. This gives us the desired contradiction.

(3) Suppose n is even. Then $f'(n) = 0$ has only one real root, namely

$$n^{-1/(n-1)}.$$

It is easily verified that $f(x) \to +\infty$ as $x \to \pm\infty$. Hence, f attains its minimum at $x = n^{-1/(n-1)}$. It is easily verified that this minimum is negative. Hence, f has two real zeros.

Now suppose n is odd. Then $f'(x) = 0$ has two real roots, namely

$$\pm n^{-1/(n-1)}.$$

Now $f(x) \to -\infty$ as $x \to -\infty$ and $f(x) \to \infty$ as $x \to \infty$, so f attains a local maximum at $-n^{-1/(n-1)}$ and attains a local minimum at $n^{-1/(n-1)}$. It is easily verified that f is negative at both these points, so f has only one real zero.

(4) It is easily verified that $f(2^{1/n}) < 0$, while $f(3^{1/n}) > 0$. Also, if n is even, then $f(-1) = 1$ but $f(0) = -1$.

(5) Let $y_0 = r_0e^{i\theta}$ be a complex zero of f. Then

$$f(y_0) = (r_0e^{i\theta})^n - r_0e^{i\theta} - 1 = 0.$$

Hence, $r_0 = |r_0e^{i\theta} + 1| < r_0 + 1$. Thus, $f(r_0) = r_0^n - r_0 - 1 < 0$. However, r_0 is positive; and from parts (3) and (4) above, we see that if r_0 is positive and $f(r_0) < 0$, then $r_0 < \alpha$. Hence, $|y_0| < \alpha$.

This completes the proof of our Theorem. □

This theorem implies that if

$$T_k = \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k,$$

and if $\alpha_1 = \alpha$, the positive real zero of $x^n - x - 1$, then the other zeros are smaller in magnitude, and hence for large k we have

$$T_k \sim \alpha^k.$$

From part (4) of the theorem, we know that

$$2^{1/n} < \alpha < 3^{1/n},$$

so by choosing n sufficiently large, we can make α as close to 1 as desired. For example, if we choose $n = 4$, we get a sequence with property (1) that grows approximately like 1.22^k.

The authors thank the referee for detailed comments and a shorter proof of part (2) of the theorem.

REFERENCES

1. L. E. Dickson. Solution to Problem 151. *Amer. Math. Monthly* 15 (1908):209.
2. E. B. Escott. Response to Question 1484. *L'Intermédiaire des Math.* 8 (1901): 63-64.
3. E. B. Escott. Problem 151. *Amer. Math. Monthly* 15 (1908):22.
4. E. Lucas. "Theorie des fonctions numériques simplement périodiques." *American J. Math.* 1 (1878):184-240.
5. E. Malo. Response to Question 1481. *L'Intermédiaire des Math.* 7 (1901):280-82, 312-24.
6. B. H. Neumann & L. G. Wilson. "Some Sequences Like Fibonacci's." *The Fibonacci Quarterly* 17 (1979):80-83.
7. R. Perrin. Question 1484. *L'Intermédiaire des Math.* 6 (1899):76-77.
8. A. G. Shannon & A. F. Horadam. "Concerning a Ppaer by L. G. Wilson." *The Fibonacci Quarterly* 20 (1982):38-41.

◆◇◆◇◆