SECOND-ORDER LINEAR RECURRENCES OF COMPOSITE NUMBERS

Lawrence Somer
Department of Mathematics, The Catholic University of America, Washington, D.C. 20064
e-mail: somer@cua.edu

(Submitted April 2005)

ABSTRACT

In a well-known result, Ronald Graham found a Fibonacci-like sequence whose two initial terms are relatively prime and which consists only of composite integers. We generalize this result to nondegenerate second-order recurrences.

1. INTRODUCTION

It is widely believed that there exist infinitely many primes in the Fibonacci sequence $\{F_n\}$ (see [4, p. 17]). In 1964 Ronald Graham [3] proved the surprising result that there exists a Fibonacci-like sequence $\{G_n\}$ satisfying $G_{n+2} = G_{n+1} + G_n$ with initial 33- and 34-digit terms G_0 and G_1 containing only composite integers (see [3] with a correction given in [6]). He found this sequence by means of a covering set of the integers. We will extend Graham's result to a very general class of second-order linear recurrences. Izotov [5] has also generalized Graham's result to a more restrictive set of second-order linear recurrences having positive discriminant.

Let $w(a, b)$ denote the second-order linear recurrence satisfying the recursion relation

$$w_{n+2} = aw_{n+1} + bw_n, \tag{1}$$

where a, b, and the initial terms $w_0,\ w_1$ are all integers. Associated with $w(a, b)$ is the characteristic polynomial

$$f(x) = x^2 - ax - b \tag{2}$$

with characteristic roots α and β and discriminant $D = a^2 + 4b = (\alpha - \beta)^2$. The recurrence $w(a, b)$ is said to be degenerate if $ab = 0$ or α/β is a root of unity. A special well-studied type of second-order recurrence is the Lucas sequence $u(a, b)$ satisfying (1) and having initial terms $u_0 = 0,\ u_1 = 1$. By the Binet formula,

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{3}$$

It follows from (3) that

$$m|n \Rightarrow u_m|u_n \tag{4}$$

and

$$u_n(-a, b) = (-1)^{n+1}u_n(a, b). \tag{5}$$

In searching for recurrences $w(a, b)$ having only composite integers as terms, it suffices to find a recurrence $w'(a, b)$ such that w'_n is composite for $n \geq N$. Then $w(a, b)$, defined by $w_n = w'_{n+N}$, contains only composite numbers, where w_n can be positive or negative.

In our subsequent discussion, we will need results about nondegenerate second-order linear recurrences. Theorem 1 was proved by Parnami and Shorey [7].

Theorem 1: Let $w(a,b)$ be a nondegenerate recurrence. Then there exists a constant N_1 such that

$$w_m \neq w_n \tag{6}$$

whenever $m \neq n$ and $\max(m,n) \geq N_1$.

We observe that the only interesting cases of nondegenerate recurrences $w(a,b)$ having only composite numbers are those in which $gcd(a,b) = gcd(w_0,w_1) = 1$. If $gcd(a,b) = d > 1$, then it can be shown by induction that $d^k | w_n$ for $n \geq 2k$. If $gcd(w_0,w_1) = d_1 > 1$, then $d_1 | w_n$ for all $n \geq 0$. By Theorem 1, there exists a positive integer N such that $|w_n| > d_1$, and hence w_n is composite for all $n \geq N$.

It is conjectured (see [4, p. 17] or [8, p. 362]) that for infinitely many ordered pairs (a,b) for which $gcd(a,b) = 1$, $u(a,b)$ is nondegenerate and $|u_n(a,b)|$ is a prime for infinitely many n. However, we shall prove the following theorem:

Theorem 2: Let $u(a,b)$ be a nondegenerate Lucas sequence for which $gcd(a,b) = 1$. Then there exists a recurrence $w(a,b)$ for which $gcd(w_0,w_1) = 1$ and w_n is composite for $n \geq 0$.

2. PRELIMINARIES

To prove Theorem 2, we will need results about covering sets and primitive prime divisors of Lucas sequences. A system of congruences $c_i \pmod{m_i}$ $(1 \leq i \leq k)$, where $0 \leq c_i < m_i$ and $2 \leq m_1 \leq m_2 \leq \cdots \leq m_k$ is a covering set for the integers if every integer y satisfies $y \equiv c_i \pmod{m_i}$ for at least one value of i. Given the Lucas sequence $u(a,b)$, p is a primitive prime divisor of u_n if $p | u_n$, but $p \not| u_i$ for $1 \leq i < n$.

Theorem 3: There exists a covering set $c_i \pmod{m_i}$ $(1 \leq i \leq k)$ of the integers such that $20 \leq m_1 < m_2 < m_3 < \cdots < m_k$.

Theorem 3 was proved by Choi [2]. In utilizing Theorem 3 in our proof of Theorem 2, we will be seeking primitive prime divisors of $u_{m_i}(a,b)$, where $m_i \geq 20$ is one of the moduli in the covering set discussed in Theorem 3. Theorem 4 below guarantees that with two exceptions, we can always find a primitive prime divisor of $u_{m_i}(a,b)$.

Theorem 4: Let $u(a,b)$ be a nondegenerate Lucas sequence for which $gcd(a,b) = 1$. Then u_n has no primitive divisor only if $n = 1,2,3,4,5,6,7,8,10,12,13,18$, or 30. Moreover, $u_{30}(a,b)$ has no primitive divisor if and only if $a = \pm 1$ and $b = -2$. In this case, $|u_{30}| = 24475 = 5^2 \cdot 11 \cdot 89$.

Theorem 4 is a special case of the results proved by Bilu, Hanrot, and Voutier in [1]. We will also need to make use of Lemma 1.

Lemma 1: Let $w(a,b)$ be a recurrence for which $gcd(a,b) = 1$ and let p be a prime such that $p | b$ and $p \not| w_1(a,b)$. Then $p \not| w_n(a,b)$ for $n \geq 1$.

Proof: This is easily proved by induction upon use of the recursion relation (1).

3. PROOF OF THE MAIN THEOREM

Proof of Theorem 2: It suffices to find a recurrence $t(a,b)$ such that $gcd(t_n, t_{n+1}) = 1$ for all $n \geq 0$ and t_n is composite for $n \geq N_1$. Then $\{w_n\}_{n=0}^{n=\infty}$ is the desired recurrence, where $w_n = t_{N_1+n}$.

By Theorem 3, there exists a covering set of the integers given by $c_i \pmod{m_i}$ $(1 \le i \le k)$, where $0 \le c_i < m_i$ and $20 \le m_1 < m_2 < \cdots < m_k$. By Theorem 4, $u_{m_i}(a,b)$ has a primitive prime divisor p_i if it is not the case that both $(a,b) = (\pm 1, -2)$ and $m_i = 30$. If $(a,b) = (\pm 1, -2)$, then we let $p_i = 5$, which divides $u_{30}(\pm 1, -2)$. Since 5 is a primitive prime divisor of $u_6(\pm 1, -2) = \pm 5$, we see that $gcd(p_i, p_j) = 1$ for $1 \le i < j \le k$.

We now define t_0 and t_1 to be integers satisfying the simultaneous system of congruences

$$\begin{aligned} &t_0 \equiv u_{m_i - c_i} \pmod{p_i},\ i = 1, 2, \ldots, k \\ &t_0 \equiv 1 \pmod{b} \\ &t_1 \equiv u_{m_i + 1 - c_i} \pmod{p_i},\ i = 1, 2, \ldots, k \\ &t_1 \equiv 1 \pmod{b}. \end{aligned} \tag{7}$$

We note that $gcd(p_i, b) = 1$ for $1 \le i \le k$ by Lemma 1, since $p_i | u_{m_i}$.

Let $P = bp_1p_2 \ldots p_k$. By the Chinese remainder theorem, there exist unique integers Q_0 and Q_1 such that $t_0 \equiv Q_0 \pmod{P}$, $t_1 \equiv Q_1 \pmod{P}$, and $0 \le Q_0,\ Q_1 < P$.

Let $d = gcd(Q_0, Q_1)$. We claim that

$$gcd(d, P) = 1. \tag{8}$$

First we observe that $gcd(d, b) = 1$, since $t_0 \equiv Q_0 \equiv 1 \pmod{b}$ and $t_1 \equiv Q_1 \equiv 1 \pmod{b}$. Suppose that $p_i | d$ for some i such that $1 \le i \le k$. Then by (7), $p_i | u_{m_i - c_i}$ and $p_i | u_{m_i - c_i + 1}$, where $m_i - c_i \ge 1$. By (1),

$$p_i | u_{m_i - c_i + 1} - a u_{m_i - c_i} = b u_{m_i - c_i - 1}.$$

Since $p_i \not| b$, we see that $p_i | u_{m_i - c_i - 1}$. Continuing in this manner, we find that $p_i | u_1$, which is a contradiction. Thus, (8) is satisfied.

If $d = 1$, we let $t_0 = Q_0$ and $t_1 = Q_1$. If $d > 1$, let g be the product of all the distinct primes dividing Q_1 but not dividing Q_0. If no such primes exist, let $g = 1$. We now define t_0 to be equal to $Q_0 + gP$ and t_1 to be equal to Q_1. Then all the simultaneous congruences in (7) still hold. Since $gcd(d, gP) = gcd(g, Q_0) = 1$, it follows that $gcd(t_0, t_1) = 1$.

We now demonstrate that for each $n \ge 0, p_i | t_n$ for some i such that $1 \le i \le k$. First note that $n = c_i + rm_i$ for some $i \in \{1,\ 2,\ \ldots,\ k\}$ and some nonnegative integer r. Since $t(a,b)$ satisfies the same recursion relation as $u(a,b)$, we see from (7) and (4) that

$$t_n = t_{c_i + rm_i} \equiv u_{(r+1)m_i} \equiv 0 \pmod{p_i}. \tag{9}$$

It now follows from Theorem 1 that there exists a positive integer N such that t_n is composite for $n \ge N$.

To complete the proof, we show that $gcd(t_n, t_{n+1}) = 1$ for $n \ge 0$. Suppose that $p | gcd(t_j, t_{j+1})$ for some $j \ge 0$ and some prime p. Then $p | t_{j+1} - at_j = bt_{j-1}$. Suppose further that $p | b$. However, $p \not| t_1$, since $t_1 \equiv 1 \pmod{b}$. Thus, by Lemma 1, $p \not| t_n$ for any $n \ge 1$, contrary to our assumption about p. Hence, $p | t_{j-1}$. Continuing, we find that $p | gcd(t_0, t_1)$, which again is a contradiction. $\square$

4. DEGENERATE RECURRENCES

For completeness, we now treat the case in which $w(a,b)$ is nondegenerate and $gcd(a,b) = gcd(w_0, w_1) = 1$. Since the characteristic polynomial is quadratic, it follows that α/β can be an mth root of unity only if $m = 1, 2, 3, 4$, or 6. If $m = 4$, then (a,b) is of the form $(2s, -2s^2)$, while if $m = 6$, then (a,b) is of the form $(3s, -3s^2)$. In neither case does $gcd(a,b) = 1$. If $m = 3$, then $(a,b) = (\pm 1, -1)$ and $|w(a,b)|$ is purely periodic with a period of 3, whereas if $m = 2$, then $(a,b) = (0, \pm 1)$ and $|w(a,b)|$ has a period of 2. In both these cases, it is easy to find recurrences $w(a,b)$ having only composite terms. If $b = 0$, then $(a,b) = (\pm 1, 0)$ and $|w(a,b)|$ is periodic for $n \geq 1$ with a period of 1. Again, it is trivial to construct sequences $w(a,b)$ having only composite numbers.

The most interesting case occurs when $\alpha/\beta = 1$. Then $D = 0$ and $(a,b) = (\pm 2, -1)$. If $(a,b) = (2,-1)$, then $w_n = w_0 + n(w_1 - w_0)$, and $w(a,b)$ is an arithmetic progression. Since $(w_0, w_1) = 1$ the common difference $w_1 - w_0$ is relatively prime to the initial term w_0. If $(w_0, w_1) = (1,1)$ or $(-1,-1)$, then $w_n = \pm 1$ for $n \geq 0$, and $w(a,b)$ has no composite terms. If $w_1 - w_0 \neq 0$, then $|w(a,b)|$ contains infinitely many primes by Dirichlet's theorem on the infinitude of primes in arithmetic progressions. Thus, there exists no recurrence $w(2,-1)$ containing only composite numbers when $gcd(w_0, w_1) = 1$.

REFERENCES

[1] Yu Bilu, G. Hanrot. "Existence of Primitive Divisors of Lucas and Lehmer Numbers." *J. Reine Angew. Math.* **539** (2001): 75-122.

[2] S. L. G. Choi. "Covering the Set of Integers by Congruence Classes of Distinct Moduli." *Math. Comp.* **25** (1971): 885-895.

[3] R. L. Graham. "A Fibonacci-like Sequence of Composite Numbers." *Math. Mag.* **37** (1964): 322-324.

[4] R. K. Guy. *Unsolved Problems in Number Theory*, 3rd ed. Springer-Verlag, Berlin, 2004.

[5] A. S. Izotov. "Second-order Linear Recurrences of Composite Numbers." *The Fibonacci Quarterly* **40.3** (2002): 266-268.

[6] D. E. Knuth. "A Fibonacci-like Sequence of Composite Numbers." *Math. Mag.* **63** (1990): 21-25.

[7] J. C. Parnami and T. N. Shorey. "Subsequences of Binary Recursive Sequences." *Acta Arith.* **40** (1982): 193-196.

[8] P. Ribenboim. *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

AMS Classification Numbers: 11B39, 11B37

✠ ✠ ✠