Divisibility Relations between Fibonacci and Lucas Numbers

Peter Hilton and Jean Pedersen

1. Introduction

Over the years, the authors have published many papers on the arithmetical properties of Fibonacci and Lucas numbers (see [2], [3], [4], and [5]). Somer [7] had already obtained deep divisibility results, of a more general nature than ours and has, just recently, carried the story even further in [8]. We gave special attention to those numbers, called Lucasian, that are divisors of Lucas numbers, but not necessarily Lucas numbers themselves.

In this paper we concentrate on divisibility relations entirely within the domain of Fibonacci numbers F_m and Lucas number L_n. Thus, we have four questions to study: for what values of m and n is F_m a divisor of F_n, L_m a divisor of L_n, F_m a divisor of L_n, and L_n a divisor of F_m. To answer these questions, we include some already published results on the $\gcd$ of corresponding pairs of numbers; that is,

$$\gcd(F_m, F_n)\,, \quad \gcd(L_m, L_n)\,, \quad \gcd(F_m, L_n)\,,$$

that are contained in Section 3. Armed with these statements, in Section 4 we obtain complete characterizations of the required divisibility results. It turns out that, in all 4 cases, there is an *initial* condition and a *general* situation. Thus, for example, in Theorem 5 we answer the question: when is F_m a divisor of F_n? The answer is that this occurs precisely in the initial situation $m = 2$ and in the general situation $m \mid n$.

Our results are stated for m and n positive. One can extend them to encompass the possibility of m or n being negative (or zero) in light of (4).

Section 2 collects together the elementary properties of Fibonacci and Lucas numbers required in the last two sections.

2. Elementary Properties

The elementary linear properties are

$$L_n \;=\; F_{n-1} + F_{n+1} \tag{2}$$

and

$$5F_n \;=\; L_{n-1} + L_{n+1}\,. \tag{3}$$

Negative values of n are included through the rules

$$F_{-n} \;=\; (-1)^{n-1}F_n\,, \quad L_{-n} \;=\; (-1)^n L_n\,, \tag{4}$$

which follow immediately from Binet's formulas:

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad L_n = \alpha^n + \beta^n, \tag{5}$$

where

$$\alpha + \beta = 1, \quad \alpha\beta = -1. \tag{6}$$

From (5), we immediately deduce

$$F_{2n} = F_n L_n. \tag{7}$$

A simple induction, based on the recurrence relation $F_{n+2} = F_n + F_{n+1}$, shows that

$$\gcd(F_m, F_{m-1}) = 1, \quad \text{for all } m \geq 1. \tag{8}$$

The Fibonacci and Lucas sequences modulo 2, starting with $m = 0$, both read

$$0, 1, 1, 0, 1, 1, \ldots$$

so that

$$F_m \text{ even} \iff L_m \text{ even} \iff 3 \mid m. \tag{9}$$

From (8) and (9), we infer that

Theorem 1 Either $\gcd(F_m, L_m) = 1$ or $\gcd(F_m, L_m) = 2$.

Remark. Obviously, here and subsequently, we have $\gcd(F_m, L_m) = 2$ if and only if $3 \mid m$.

Proof:

$$\begin{aligned} \gcd(F_m, L_m) &= \gcd(F_m, F_{m-1} + F_{m+1}), \quad \text{by (2)} \\ &= \gcd(F_m, F_m + 2F_{m-1}), \quad \text{by the recurrence relation} \\ &= \gcd(F_m, 2F_{m-1}) \\ &= 1 \text{ or } 2, \quad \text{by (8) and (9).} \end{aligned}$$

■

Finally, Binet's formulas, together with (6), make it plain that

$$F_m \mid F_n \quad \text{if } m \mid n \tag{10}$$

and

$$L_m \mid L_n \quad \text{if } m \mid n \text{ oddly.} \tag{11}$$

(Recall that $a \mid b$ oddly means that b/a is an odd integer.)

3. The gcd Theorems

In this section we recall the three key gcd theorems relating to the sequences $\{F_n\}$ and $\{L_n\}$. Throughout the rest of this paper m and n are positive integers, $d = \gcd(m, n)$, and $|m|_2 = \max\{\mu : 2^\mu \mid m\}$. We will allow ourselves to consider F_m and L_m with negative (or zero) values of m, but never in the statements of our theorems. The three theorems are:

Theorem 2 $\gcd(F_m, F_n) = F_d$.

Theorem 3 $\gcd(L_m, L_n) = \begin{cases} L_d & \text{if } |m|_2 = |n|_2, \\ 1 \text{ or } 2 & \text{otherwise.} \end{cases}$

Theorem 4 $\gcd(F_m, L_n) = \begin{cases} L_d & \text{if } |m|_2 > |n|_2, \\ 1 \text{ or } 2 & \text{otherwise.} \end{cases}$

An elementary proof of Theorem 2 may be found in [1], Theorem 13.3. We do not know of any elementary proof of Theorem 3 or Theorem 4, whose statements are obviously more subtle than that of Theorem 2. Proofs of Theorems 3 and 4 may be found in [2] and [6].

4. The Divisibility Properties

Theorem 5 $F_m \mid F_n$ if and only if $m = 2$ or $m \mid n$.

Proof: The divisibility statement that $F_m \mid F_n$ if $m \mid n$ is (10). Since $F_2 = 1$, it is trivial that $F_m \mid F_n$ if $m = 2$. Now suppose $F_m \mid F_n$. We will assume that $m \geq 3$, since $F_1 = F_2 = 1$, and it is obvious that $m \mid n$ if $m = 1$.

By Theorem 2, $F_m = F_d$ if $F_m \mid F_n$. But F_m strictly increases with m if $m \geq 2$; thus, if $m \geq 3$ and $F_m \mid F_n$, then $m = d$; that is, $m \mid n$. ∎

Theorem 6 $L_m \mid L_n$ if and only if $m = 1$ or $m \mid n$ oddly.

Proof: The statement that $L_m \mid L_n$ if $m \mid n$ oddly is (11). Since $L_1 = 1$, it is obvious that $L_m \mid L_n$ if $m = 1$. Now suppose that $L_m \mid L_n$ and $m \neq 1$. Then $\gcd(L_m, L_n) = L_m$ and $L_m \geq 3$. Hence, by Theorem 3, $|m|_2 = |n|_2$ and $L_m = L_d$. But L_m is strictly increasing with m (for m positive). Hence, $m = d$; that is, $m \mid n$. But since $|m|_2 = |n|_2$, it follows that $m \mid n$ oddly. ∎

We now come to the most interesting, and surprising, results.

Theorem 7 $F_m \mid L_n$ if and only if one of the following holds:

(i) $m = 1$,

(ii) $m = 2$,

(iii) $m = 3$ and $3 \mid n$, or

(iv) $m = 4$ and $n \equiv 2 \pmod 4$.

Proof: We first show that, if $F_m \geq 3$ and F_m divides some L_n, then $F_m = 3$. To prove this, we start by making the stronger hypothesis that $F_m \geq 3$ and $F_m = L_n$, for some n. Then $\gcd(F_m, L_n) = F_m = L_n \geq 3$. Thus, by Theorem 4, we have $|m|_2 > |n|_2$ and $F_m = L_n = L_d$. Since L_n is strictly increasing, we see that $n = d$, implying that $n \mid m$. But since $|m|_2 > |n|_2$, one has $2n \mid m$. Thus,

$$L_n \mid F_{2n} \mid F_m \,.$$

But $L_n = F_m$. Then $L_n = F_{2n}$; whence $F_n = 1$, implying that $n = 1$ or 2. But it is not possible that $n = 1$, since $L_1 = 1 < 3$. Therefore, $n = 2$ and $F_m = L_2 = 3$.

Now assume only that $F_m \mid L_n$ with $F_m \geq 3$. Then we have $\gcd(F_m, L_n) = F_m \geq 3$. Hence, by Theorem 4, we see that $|m|_2 > |n|_2$ and $F_m = L_d$. But we have already shown that $F_m = L_d \geq 3$ implies that $F_m = 3$.

Thus, the condition $F_m \mid L_n$ implies that $F_m \leq 3$; that is, $m \leq 4$. Of course, $F_m \mid L_n$ if $m = 1$ or 2. Assume now that $m = 3$. Then $F_3 = 2$. Hence, $F_3 \mid L_n$ if and only if L_n is even; that is, $3 \mid n$.

Finally, suppose $m = 4$. Since $F_4 = 3$, we know that $F_m \mid L_n$ if and only if $3 \mid L_n$. But the Lucas sequence modulo 3, starting with $n = 1$, reads

$$1\,,\,0\,,\,1\,,\,1\,,\,2\,,\,0\,,\,2\,,\,2\,,\,1\,,\,0\,,\;\ldots$$

Therefore, $3 \mid L_n$ if and only if $n \equiv 2 \pmod 4$.

This completes the proof of Theorem 7. ■

Our final theorem is

Theorem 8 $L_n \mid F_m$ if and only if $n = 1$ or $2n \mid m$.

Proof: If $n = 1$, then $L_n = 1$, and $L_n \mid F_m$. If $2n \mid m$, then $L_n \mid F_{2n} \mid F_m$ by (7) and (10). Conversely, suppose $L_n \mid F_m$, for $n \neq 1$. Then $L_n \geq 3$ and $\gcd(F_m, L_n) = L_n$. It follows from Theorem 4 that $L_n = L_d$ and $|m|_2 > |n|_2$. Since L_n is a strictly increasing function of n, we have $n = d$; that is, $n \mid m$. But $|m|_2 > |n|_2$, so, in fact, $2n \mid m$. ■

Theorems 5 and 8 have the following rather striking consequence.

Corollary 1 $L_n \mid F_m$ if and only if $F_{2n} \mid F_m$.

Proof: Both divisibility conditions are equivalent to $n = 1$ or $2n \mid m$. ■

Of course, it is obvious from (7) that $L_n \mid F_m$ if $F_{2n} \mid F_m$; it is the converse implication which is somewhat surprising. Indeed, the corollary itself has the consequence that $F_n \mid F_m$ if $L_n \mid F_m$, itself rather striking since, by Theorem 1, F_n and L_n are 'nearly' coprime.

This may also be seen by noting that $3 = L_2$ and we know, by Theorem 6, that $L_2 \mid L_n$ if and only if $2 \mid n$ oddly; that is, $n \equiv 2 \pmod 4$.

References

[1] Burton, David, *Elementary Number Theory*, 5th edition, McGraw-Hill, 2002.

[2] Hilton, Peter, and Jean Pedersen, Fibonacci and Lucas numbers in teaching and research, *Journées Mathématiques & Informatique*, Vol. 3 (1991–1992), 36–57.

[3] Hilton, Peter, Derek Holton, and Jean Pedersen, *Mathematical Reflections – In a Room with Many Mirrors*, Undergraduate Texts in Mathematics, Springer–Verlag, New York, 1997, 351 pp. (Second printing, 1998.)

[4] Hilton, Peter, Derek Holton, and Jean Pedersen, *Mathematical Vistas – In a Room with Many Mirrors*, Undergraduate Texts in Mathematics, Springer–Verlag, New York, 2002, 335 pp.

[5] Hilton, Peter, Jean Pedersen, and Lawrence Somer, On Lucasian numbers, *The Fibonacci Quarterly*, 35(1), (1997), 43–47.

[6] McDaniel, Wayne, The gcd in Lucas sequences and Lehmer number sequences, *The Fibonacci Quarterly*, 29(1), (1991), 24–29.

[7] Somer, Lawrence, Divisibility of terms in Lucas sequences by their subscripts, G.E. Bergum et al. (eds), *Applications of Fibonacci Numbers*, 5, Kluwer Academic Publishers (1993), 515–525.

[8] Somer, Lawrence, A further note on Lucasian numbers, F.T. Howard (ed.), *Applications of Fibonacci Numbers*, 9: Proceedings of the Tenth International Research Conference on Fibonacci numbers and their Applications. Kluwer Academic Publishers (2004), 225–234.

Peter Hilton
Department of Mathematical Sciences
State University of New York
Binghamton, NY 13902-6000
USA

Jean Pedersen
Department of Mathematics and Computer Science
Santa Clara University
Santa Clara, CA 95053-0290
USA
jpedersen@scu.edu