DIVISIBILITY BY FIBONACCI AND LUCAS SQUARES

V. E. HOGGATT, JR., and MARJORIE BICKNELL JOHNSON
San Jose State University, San Jose, California 95192

1. INTRODUCTION

In Matijasevic's paper [1] on Hilbert's Tenth Problem, Lemma 17 states that F_m^2 divides F_{mr} if and only if F_m divides r. Here, we extend Lemma 17 to its counterpart in Lucas numbers and generalized Fibonacci numbers and explore divisibility by higher powers.

In [2], Matijasevic's Lemma 17 was proved by Hoggatt, Phillips and Leonard using an identity for F_{mr}. Since that proof is the basis for our extended results, we repeat it here.

We let $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$. Then it is well known that the Fibonacci numbers F_n are given by

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{1.1}$$

and that

$$\alpha^m = \alpha F_m + F_{m-1}, \qquad \beta^m = \beta F_m + F_{m-1}. \tag{1.2}$$

Combining (1.1) and (1.2) with the binomial theorem expansion of α^{mr} and β^{mr} gives

$$F_{mr} = \frac{\alpha^{mr} - \beta^{mr}}{\alpha - \beta} = \sum_{k=0}^{r} \binom{r}{k} F_m^k F_{m-1}^{r-k} \left(\frac{\alpha^k - \beta^k}{\alpha - \beta} \right)$$

so that

$$F_{mr} = \sum_{k=0}^{r} \binom{r}{k} F_m^k F_{m-1}^{r-k} F_k . \tag{1.3}$$

Since $F_0 = 0$ and F_m^2 divides all terms for $k \geq 2$,

$$F_{mr} \equiv \binom{r}{1} F_m F_{m-1}^{r-1} F_1 \equiv r F_m F_{m-1}^{r-1} \pmod{F_m^2} .$$

Since $(F_m, F_{m-1}) = 1$, it follows easily that

$$F_m^2 \mid F_{mr} \quad \text{if and only if} \quad F_m \mid r. \tag{1.4}$$

2. DIVISIBILITY BY OTHER FIBONACCI POWERS

The proof of (1.4) can easily be extended to give results for divisibility by higher powers.

Since F_m^3 divides all terms of (1.3) for $k \geq 3$, and since $F_1 = F_2 = 1$, proceeding in a manner similar to that of Section 1,

$$F_{mr} \equiv r F_m F_{m-1}^{r-1} + \frac{r(r-1)}{2} F_m^2 F_{m-1}^{r-2} \pmod{F_m^3} .$$

When r is odd, $(r-1)/2 = k$ is an integer, and

$$F_{mr} \equiv r F_m F_{m-1}^{r-2} (F_{m-1} + k F_m) \pmod{F_m^3} .$$

Since $(F_m, F_{m-1}) = 1$,

$$F_m \nmid (F_{m-1} + k F_m) \qquad \text{and} \qquad F_m \nmid F_{m-1}^{r-2},$$

so that $F_m^3 \mid F_{mr}$ if and only if $F_m^2 \mid r$.

If r is even,

$$F_{mr} \equiv \frac{r}{2} F_m F_{m-1}^{r-2}(2F_{m-1} + (r-1)F_m) \pmod{F_m^3}.$$

If $(F_m, 2F_{m-1}) = 1$, then $F_m^3 | F_{mr}$ if and only if $F_m^2 | r$. Thus, we have proved

Theorem 2.1. Whenever r is odd, $F_m^3 | F_{mr}$ iff $F_m^2 | r$. Whenever F_m is odd, $F_m^3 | F_{mr}$ iff $F_m^2 | r$.

Sinilarly, since $F_1 = F_2 = 1$ and $F_3 = 2$, from (1.3) we can write

$$F_{mr} \equiv rF_m F_{m-1}^{r-1} + \frac{r(r-1)}{2} F_m^2 F_{m-1}^{r-2} + \frac{r(r-1)(r-2)}{3} F_m^3 F_{m-1}^{r-3} \pmod{F_m^4}$$

since F_m^4 divides every term for $k \geq 4$.

If $r = 6k \pm 1$, then $(r-1)/2 = j$ and $(r-1)(r-2)/3 = i$ for integers j and i, so that

$$F_{mr} \equiv rF_m F_{m-1}^{r-3}(F_{m-1}^2 + jF_m F_{m-1} + iF_m^2) \pmod{F_m^4}.$$

As before, since $(F_m, F_{m-1}) = 1$, $F_m^4 | F_{mr}$ iff $F_m^3 | r$, $r = 6k \pm 1$.

If $r = 6k$, then

$$F_{mr} \equiv \frac{r}{6} F_m F_{m-1}^{r-1}(6F_{m-1}^2 + 3(r-1)F_m F_{m-1} + 2(r-1)(r-2)F_m^2) \pmod{F_m^4}.$$

If $(F_m, 6F_{m-1}^2) = 1$, then $F_m^4 | F_{mr}$ iff $F_m^3 | \frac{r}{6}$. Note that $(F_m, 6) = 1$ if $m \neq 3q$, $m \neq 4q$. The cases $r = 6k \pm 2$ and $r = 6k \pm 3$ are similar. Thus, we have proved

Theorem 2.3. Whenever $r = 6k \pm 1$, $F_m^4 | F_{mr}$ iff $F_m^3 | r$. Whenever $m \neq 3q$, $m \neq 4q$, $F_m^4 | F_{mr}$ iff $F_m^3 | r$.

Continuing in a similar fashion and considering the first terms generated in the expansion of F_{mr}, we could prove that whenever $r = 6k \pm 1$, or $m \neq 3q, 4q$,

$$F_m^5 | F_{mr} \text{ iff } F_m^4 | r, \qquad \text{and also} \qquad F_m^6 | F_{mr} \text{ iff } F_m^5 | r,$$

but the derivations are quite long. In the general case, again considering the first terms of (1.3), we can state that, whenever $r = k(s-1)! \pm 1$, $F_m^s | F_{mr}$ iff $F_m^{s-1} | r$, by carefully considering the common denominator of the fractions generated from the binomial coefficients.

We summarize these cases in the theorem below.

Theorem 2.4. Whenever $r = 6k \pm 1$,

$$F_m^s | F_{mr} \text{ iff } F_m^{s-1} | r, \quad s = 1, 2, 3, 4, 5, 6.$$

Whenever $m \neq 3q$, $m \neq 4q$,

$$F_m^s | F_{mr} \text{ iff } F_m^{s-1} | r, \quad s = 1, 2, 3, 4, 5, 6.$$

Whenever $r = k(s-1)! \pm 1$,

$$F_m^s | F_{mr} \text{ iff } F_m^{s-1} | r.$$

Next, we make use of a Lemma to prove a final theorem for the general case.

Lemma. If $s^{n-1} | r$, then $s^{nk} | \binom{r}{k}$, $k = 1, \cdots, n$.

Proof. If $n \leq r$, then $k \leq n \leq r$. Cases $k = 1$ and $k = r$ are trivial. Case $s = 1$ is trivial. If $s^{n-1} | r$, then $r = Ms^{n-1}$ for some integer M, and

$$\binom{r}{k} = \frac{r}{k}\binom{r-1}{k-1} = \frac{Ms^{n-1}}{k}\binom{r-1}{k-1} = \frac{Ms^{k-1}s^{n-k}}{k}\binom{r-1}{k-1}.$$

If

$$k | Ms^{k-1}\binom{r-1}{k-1},$$

then

$$s^{n-k} | \binom{r}{k}.$$

If

$$k \nmid Ms^{k-1}\binom{r-1}{k-1},$$

then

$$k \mid Ms^q \binom{r-1}{k-1}, \quad k \leq q \leq n,$$

since $\binom{r}{k}$ is an integer. That is, $k = p^q N$, where p is some prime.

But $k < p^q$ for $p \geq 2$ and $q \geq k \geq 0$, a contradiction, so that k must divide

$$Ms^{k-1}\binom{r-1}{k-1}, \quad \text{and} \quad s^{n-k} \Big| \binom{r}{k}.$$

It is impossible for $n > r$. If $n < r$, then $s^{n-1} | r$ implies $Ms^{n-1} = r$, where $n - 1 \geq r$, and where M is an integer. But $s^{n-1} > r$ for $s \geq 2$, $n - 1 \geq r$.

Theorem. If $F_m^{s-1} | r$, then $F_m^s | F_{mr}$.

Proof.

$$F_{mr} = \sum_{k=0}^{r} \binom{r}{k} F_m^k F_{m-1}^{r-k} F_k .$$

If $k \geq s$, then F_m^s divides each term. Since $F_0 = 0$, F_m^s divides the term $k = 0$. When $k = 1$, the term is $rF_m F_{m-1}^{r-1}$. $(F_m, F_{m-1}) = 1$, so that if $F_m^{s-1} | r$, then F_m^s divides $rF_m F_{m-1}^{r-1}$. If F_m^{s-1} divides r, then F_m^{s-k} divides $\binom{r}{k}$ for $k = 1, \cdots, s$ by the Lemma, and F_m^s divides each successive term for $k = 1, \cdots, s$, since in the k^{th} term we always have a factor F_m^k while F_m^{s-k} appears as a factor of $\binom{r}{k}$.

These theorems allow us to predict the entry point of F_m^k in the Fibonacci sequence in limited circumstances. The entry point of a number n in the Fibonacci sequence is the subscript of the first Fibonacci number of which n is a divisor. When $m \neq 3j$ or $4j$, the entry point of F_m^k in the Fibonacci sequence is mF_m^{k-1} for $k = 1, 2, 3, 4, 5,$ or 6.

3. DIVISIBILITY BY LUCAS SQUARES

Next, we will derive and extend the counterpart of (1.4) for the Lucas numbers. It is well known that, analogous to (1.1), the Lucas numbers L_n obey

$$L_n = \alpha^n + \beta^n \tag{3.1}$$

and

$$\alpha^m = \frac{L_m + \sqrt{5}F_m}{2}, \qquad \beta^m = \frac{L_m - \sqrt{5}F_m}{2}. \tag{3.2}$$

Combining (3.1) and (3.2) with the binomial theorem expansion of α^{mr} and β^{mr},

$$L_{mr} = \alpha^{mr} + \beta^{mr} = \left(\frac{L_m + \sqrt{5}F_m}{2}\right)^r + \left(\frac{L_m - \sqrt{5}F_m}{2}\right)^r$$

$$= (\tfrac{1}{2})^r \sum_{j=0}^{r} \binom{r}{j} L_m^{r-j} F_m^j (\sqrt{5})^j [1 + (-1)^j].$$

When j is odd, all terms are zero. We let $j = 2i$ and simplify to write

$$L_{mr} \cdot 2^{r-1} = \sum_{i=0}^{[r/2]} \binom{r}{2i} L_m^{r-2i} F_m^{2i} \cdot 5^i . \tag{3.3}$$

All terms on the right of (3.3) are divisible by L_m^2 except the last term, $i = [r/2]$. If $r = 2t$, the last term is

$$\binom{2t}{2t} L_m^0 F_m^{2t} 5^t = 5^t F_m^{2t}.$$

Since $5 \nmid L_m$ for any m and $L_m \nmid F_m$ for any $m > 1$, $L_m^2 \nmid 2^{r-1}L_{mr}$, $m > 1$. However, if $r = 2t + 1$, the last term is

$$\binom{2t+1}{2t} L_m F_m^{2t} 5^t = (2t+1)5^t L_m F_m^{2t},$$

and $2^{2t}L_{(2t+1)m}$ is divisible by L_m^2 if and only if $L_m \mid (2t+1)$, $m > 1$. If $m \neq 3q$, then $(L_m, 2) = 1$, and $L_m^2 \mid L_{m(2t+1)}$ if and only if $L_m \mid (2t+1)$. If $m = 3q$, then L_m is even, so that

$$L_m \nmid (2t+1), \qquad \text{and} \qquad L_m^2 \nmid 2^{2t}L_{(2t+1)m}, \qquad m > 1.$$

Return to (3.3) and notice that, when $r = 2t + 1$, all terms except the last are divisible by L_m^3, so that

$$L_m^3 \mid L_{mr} \text{ iff } L_m^2 \mid (2t+1), \qquad m > 1.$$

We summarize these results as

Theorem 3.1. Whenever r is odd,

$$L_m^2 \mid L_{mr} \text{ iff } L_m \mid r, \qquad \text{and} \qquad L_m^3 \mid L_{mr} \text{ iff } L_m^2 \mid r.$$

Whenever r is even, $L_m^2 \nmid L_{mr}$, $m > 1$. If $m = 3q > 1$, then $L_m^2 \nmid L_{mr}$ for any r.

We can also determine criteria for divisibility of L_{mr} by F_m^2 and F_{mr} by L_m^2. It is trivial that $F_m^2 \nmid L_{mr}$ for $m \neq 1, 2, 3, 4$, since $F_m \nmid L_n$ for other values of m. To determine when $L_m^2 \mid F_{mr}$, return to (3.1) and (3.2), and use (1.1) and the binomial expansion of α^{mr} and β^{mr} to write an expression for F_{mr} in terms of L_m. (Recall that $\sqrt{5} = \alpha - \beta$.)

$$\sqrt{5}F_{mr} = \alpha^{mr} - \beta^{mr} = \left(\frac{L_m + \sqrt{5}F_m}{2}\right)^r - \left(\frac{L_m - \sqrt{5}F_m}{2}\right)^r$$

$$= (\tfrac{1}{2})^r \sum_{j=0}^{r} \binom{r}{j} L_m^{r-j} F_m^j (\sqrt{5})^j [1 - (-1)^j].$$

Here, whenever j is even, all terms are zero. Setting $j = 2i + 1$ and rewriting, we obtain

$$\sqrt{5}F_{mr} = (\tfrac{1}{2})^r \sum_{i=0}^{[r/2]} \binom{r}{2i+1} L_m^{r-2i-1} F_m^{2i+1} \cdot (\sqrt{5})^{2i+1} \cdot 2$$

$$2^{r-1}F_{mr} = \sum_{i=0}^{[r/2]} \binom{r}{2i+1} L_m^{r-2i-1} F_m^{2i+1} \cdot 5^i. \tag{3.4}$$

Notice that, when $r = 2t + 1$, L_m^2 divides all terms of (3.4) for $i < [r/2]$. When $i = [r/2] = t$, the last term is

$$\binom{2t+1}{2t+1} L_m^0 F_m^{2t+1} \cdot 5^t = 5^t F_m^{2t+1},$$

which is not divisible by L_m, $m > 1$, since $L_m \nmid F_m$, $m > 1$, and $L_m \nmid 5^t$ for any $t > 0$. That is, if r is odd, $L_m^2 \nmid F_{mr}$ for any $m > 1$.

However, when r is even, L_m^2 divides all terms of (3.4) for $i < [r/2] - 1$. If $r = 2t$, then the terms $i = t - 1$ and $i = t$ give

$$\binom{2t}{2t-1} L_m F_m^{2t-1} 5^{t-1} + \binom{2t}{2t+1} L_m^{-1} F_m^{2t+1} 5^t = (2t) L_m F_m^{2t-1} 5^{t-1} + 0.$$

Now,

$$L_m \nmid F_m, \quad m > 1, \qquad \text{and} \qquad L_m \nmid 5^{t-1}, \quad t > 1.$$

Thus, $L_m^2 \mid 2^{2t-1}F_{m(2t)}$ if and only if $L_m \mid 2t$. If L_m is odd,

$$L_m^2 \mid F_{2mt} \text{ iff } L_m \mid t, \qquad \text{or,} \qquad L_m^2 \mid F_{mr} \text{ iff } L_m \mid r.$$

The same result holds for L_m even, which case depends upon the fact that 4 is the largest power of 2 that

divides the Lucas sequence. If L_m is even, $m = 3q$. If m is even, L_m contains exactly one factor of 2, while $F_{mr} = F_{(3q)(2t)} = F_{6t}$ contains at least three factors of 2, since $F_6 = 2^3$ is a factor of F_{6t}. If $m = 3q$ is odd, then L_m contains exactly two factors of 2, and $L_m \mid 2t$ iff $t = 2s$ for some integer s, making $F_{mr} = F_{12qs}$, a multiple of $F_{12} = 144 = 2^4 \cdot 3^2$. Thus, for L_m even, if $L_m^2 \mid 2^{r-1}F_{mr}$, then $L_m^2 \mid F_{mr}$.

Notice that, since also L_m^3 divides all terms of (3.4) for r even and $i < [r/2] - 1$, it can be shown in the same manner that

$$L_m^3 \mid F_{mr} \text{ iff } L_m^2 \mid r, \qquad \text{or,} \qquad L_m^3 \mid F_{2mt} \text{ iff } L_m^2 \mid t.$$

We summarize these results as follows.

Theorem 3.2. If r is even,

$$L_m^2 \mid F_{mr} \text{ iff } L_m \mid r, \qquad \text{and} \qquad L_m^3 \mid F_{mr} \text{ iff } L_m^2 \mid r.$$

Further,

$$L_m^2 \mid F_{2mt} \text{ iff } L_m \mid t \qquad \text{and} \qquad L_m^3 \mid F_{2mt} \text{ iff } L_m^2 \mid t.$$

If r is odd, $L_m^2 \nmid F_{mr}$, $m > 1$.

4. GENERALIZED FIBONACCI NUMBERS

The Fibonacci polynomials $f_n(x)$ are defined by

$$f_0(x) = 0, \qquad f_1(x) = 1, \qquad f_{n+1}(x) = xf_n(x) + f_{n-1}(x),$$

and the Lucas polynomials $L_n(x)$ by

$$L_0(x) = 2, \qquad L_1(x) = x, \qquad L_{n+1}(x) = xL_n(x) + L_{n-1}(x).$$

Since (1.3) is also true if we replace F_n by $f_n(x)$ (see [2]), we can write

$$f_{mr}(x) = \sum_{k=0}^{r} \binom{r}{k} f_m^k(x) f_{m-1}^{r-k}(x) f_k(x). \tag{4.1}$$

Notice that $F_m = f_m(1)$ and $L_m = L_m(1)$. The Pell numbers 1, 2, 5, 12, 29, 70, $\cdots$, P_n, $\cdots$, $P_{n+1} = 2P_n + P_{n-1}$, are given by $P_n = f_n(2)$. Thus, (4.1) also holds for Pell numbers, which leads us to

Theorem 4.1. For the Pell numbers P_n, $P_m^2 \mid P_{mr}$ iff $P_m \mid r$.

Similarly, since (3.3) and (3.4) hold for Lucas and Fibonacci polynomials, if the Lucas-analogue R_n of the Pell numbers is given by $R_n = P_{n+1} + P_{n-1}$, then $L_n(2) = R_n$, and we can write, eventually,

Theorem 4.2. If r is odd, $R_m^2 \mid R_{mr}$ iff $R_m \mid r$. If r is even, $R_m^2 \mid P_{mr}$ iff $R_m \mid r$.

We could write similar theorems for other generalized Fibonacci numbers arising from the Fibonacci polynomials.

5. DIVISIBILITY BY FIBONACCI PRIMES

From [3], [4] we know that a prime $p \mid F_{p-1}$ or $p \mid F_{p+1}$ depending upon if $p = 5k \pm 1$ or $p = 5k \pm 2$. For example, $13 \mid F_{14}$, but, note that the prime 13 enters the Fibonacci sequence earlier than that, since $F_7 = 13$. From $p \mid F_{p\pm1}$ one can easily show that $p^2 \mid F_{p^2\pm p}$, but squares of primes which are also Fibonacci numbers divide the sequence earlier than that; i.e., $F_7 = 13$, and $13^2 \mid F_{91} = F_{7 \cdot 13}$, where of course, $F_{7 \cdot 13} < F_{13^2+13}$. If p is a Fibonacci prime, if $p^2 = F_m^2 \mid F_{mr}$ then $p \mid r$ and the smallest such r is p itself, so that $p^2 \mid F_{mp}$. If $p = F_m$, then $m < p \pm 1$ since $F_{p\pm1} > p$ for $p > 5$. Thus, $F_{mp} < F_{p^2\pm p}$.

Are there other primes than Fibonacci primes for which $p^2 \mid F_n$, $n < p(p \pm 1)$?

REFERENCES

1. Yu V. Matijasevič, "Enumerable Sets are Diophantine," *Proc. of the Academy of Sciences of the USSR,* Vol. 11 (1970), No. 2.
2. V. E. Hoggatt, Jr., John W. Phillips, and H. T. Leonard, Jr., "Twenty-Four Master Identities," *The Fibonacci Quarterly,* Vol. 9, No. 1 (Feb. 1971), pp. 1–17.
3. V.E. Hoggatt, Jr., and Marjorie Bicknell, "Some Congruences of the Fibonacci Numbers Modulo a Prime p," *Mathematics Magazine,* Vol. 47, No. 4 (September-October 1974), pp. 210–214.
4. G.H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* 4th Ed., Oxford University Press, 1960.

★★★★★★★

LETTER TO THE EDITOR

March 20, 1974

Dear Sir:

I would like to contribute a note, letter, or paper to your publication expanding the topic presented below.

Following is a sequence of right triangles with integer sides, the smaller angles approximating 45 degrees as the sides increase:

(1) $$3, 4, 5, -21, 20, 29 - 119, 120, 169 - \cdots.$$

Following is another sequence of such "Pythagorean" triangles, the smallest angle approximating 30 degrees as the sides increase:

(2) $$15, 8, 17 - 209, 120, 241 - 2911, 1680, 3361 - 23408, 40545, 46817 - 564719, 326040, 652081 \cdots$$

The scheme for generating these sequences resembles that for generating the Fibonacci sequence 1, 2, 3, 5, and so on.

Let g_k and g_{k-1} be any two positive integers, $g_k > g_{k-1}$. Then, as is well known,

(3) $$g_k^2 - g_{k-1}^2, \qquad 2g_k g_{k-1}, \quad \text{and} \quad g_k^2 + g_{k-1}^2$$

are the sides of a Pythagorean triangle.

Now let m and n be two integers, non-zero, and let

(4) $$g_{k+1} = ng_k + mg_{k-1}$$

to create a sequence of g's.

If $g_1 = 1, g_2 = 2, m = 1, n = 2,$ substitution in (4) and (3) gives the triangle sequence in (1) above.

If $g_1 = 1, g_2 = 4, m = -1, n = 4,$ the resulting triangle sequence is (2) above.

If the Fibonacci sequence itself is used $(m = n = 1),$ a triangle sequence results in which the ratio between the short sides approximates 2:1.

In general, it is possible by this means to obtain a sequence of Pythagorean triangles in which the ratio of the legs, or of the hypotenuse to one leg, approximates any given positive rational number p/q (p and q positive non-zero integers, $p \geq q$). It is easy to obtain m and n and good starting values g_1 and g_2 given p/q, and there is more to the topic besides, but I shall leave all that for another communication.

For all I know, this may be an old story, known for centuries.

However, Waclaw Sierpinski, in his monograph *Pythagorean Triangles* (Scripta Mathematica Studies No. 9, Graduate School of Science, Yeshiva University, New York, 1962), does not give this method of obtaining such triangle sequences, unless I missed it in a hasty reading. He obtains sequence (1) above by a different method (Chap. 4). He shows also how to obtain Pythagorean triangles having one angle arbitrarily close to any given angle in the first quadrant (Chap. 13); but again, the method differs from the one I have outlined.

[Continued on page 10.]