DIVISIBILITY AND CONGRUENCE RELATIONS

VERNER E. HOGGATT, JR.
San Jose State University, San Jose, California 95192
and
GERALD E. BERGUM
South Dakota State University, Brookings, South Dakota 57006

In [1], we find three well known divisibility properties which exist between the Fibonacci and Lucas numbers. They are

$$F_n \mid F_m \quad \text{iff} \quad m = kn\,; \tag{1}$$

$$L_n \mid F_m \quad \text{iff} \quad m = 2kn, \quad n > 1\,; \tag{2}$$

$$L_n \mid L_m \quad \text{iff} \quad m = (2k-1)n, \quad n > 1\,. \tag{3}$$

The primary intention of this paper is to investigate the decomposition of Fibonacci and Lucas numbers in that we are interested in finding n such that $n|F_m$ or $n|L_m$. As a result of this investigation, we will also illustrate several interesting congruence relationships which exist between the elements of the sequences $\{F_n\}$ and $\{L_n\}$.

The first result, due to Hoggatt, is

Theorem 1. If $n = 2\cdot 3^k$, $k \ge 1$, then $n|L_n$.

Proof. Using α and β as the roots of the equation $x^2 - x - 1 = 0$ and recalling that $L_n = \alpha^n + \beta^n$, we have

$$\begin{aligned} L_{3n} &= \alpha^{3n} + \beta^{3n} \\ &= (\alpha^n + \beta^n)(\alpha^{2n} - \alpha^n\beta^n + \beta^{2n}) \\ &= L_n(L_{2n} - (-1)^n) = L_n(L_{2n} - 1)\,. \end{aligned}$$

However, $L_n^2 = L_{2n} + 2$ if n is even so that

$$L_{3n} = L_n(L_n^2 - 3)\,. \tag{4}$$

The theorem is true if $k = 1$ because $n = 6$ and $L_6 = 18$. The result now follows by induction on k together with (4).

Curiosity leads one to ask if there are other sequences $\{n_k\}$ such that $n_k|L_{n_k}$. The authors were unable to find other such sequences until they obtained the computer results of Mr. Joseph Greener from which they were able to make several conjectures and establish several results. Before stating the results, we establish the following theorem which was discovered independently by Carlitz and Bergum.

Theorem 2. If p is an odd prime and $p|L_n$ then $p^k|L_{np^{k-1}}$, $k \geq 1$.

Proof. By hypothesis, the theorem is true for $k = 1$. Assume $p^k|L_{np^{k-1}}$ and let $t = p^{k-1}$ then $pt|L_{nt}$. We shall show that $p^2t|L_{npt}$.

Using the factorization of $x^p + y^p$, we have

$$L_{npt} = (\alpha^{nt})^p + (\beta^{nt})^p = L_{nt}\left(\sum_{i=1}^{p} (-1)^{i+1}\alpha^{nt(p-i)}\beta^{nt(i-1)}\right) . \tag{5}$$

The middle term of the summation is

$$(-1)^{(p+3)/2}(\alpha\beta)^{nt(p-1)/2} = (-1)^{(n+1)(p-1)/2} . \tag{6}$$

The sum of the q^{th} and $(p + 1 - q)^{th}$ terms, where $q \neq (p + 1)/2$, is

$$\begin{aligned}(-1)^{q+1}\alpha^{nt(p-q)}\beta^{nt(q-1)} &+ (-1)^{p-q}\alpha^{nt(q-1)}\beta^{nt(p-q)} \\ &= (-1)^{q+1}(\alpha\beta)^{nt(q-1)}(\alpha^{nt(p-2q+1)} + \beta^{nt(p-2q+1)}) \\ &= (-1)^{(n+1)(q-1)} L_{nt(p-2q+1)} .\end{aligned} \tag{7}$$

Using (6) and (7) in (5) with $p = 4k + 1$, we have

$$\begin{aligned} L_{npt} &= L_{nt}\left(\sum_{q=1}^{2k} (-1)^{(n+1)(q-1)}L_{nt(4k-2q+2)} + 1\right) \\ &= L_{nt}\left(\sum_{q=0}^{k-1} L_{4nt(k-q)} + \sum_{q=1}^{k}(-1)^{n+1}L_{2nt(2k-2q+1)} + 1\right) \\ &= L_{nt}\left(\sum_{q=0}^{k-1} [5F^2_{2nt(k-q)} + 2] + \sum_{q=1}^{k} (-1)^{n+1}[L^2_{nt(2k-2q+1)} - 2(-1)^n] + 1\right) \\ &= L_{nt}\left(\sum_{q=0}^{k-1} 5F^2_{2nt(k-q)} + \sum_{q=1}^{k} (-1)^{n+1}L^2_{nt(2k-2q+1)} + p\right)\end{aligned} \tag{8}$$

since $L_{4r} = 5F^2_{2r} + 2$, $L^2_r = L_{2r} + 2(-1)^r$, and $t(2k - 2q + 1)$ is odd.

Now $pt|L_{nt}$, $(2k - 2q + 1)$ is odd, and $2(k - q)$ is even so that by (2) and (3) one sees that p is a factor of the expression in the parentheses of (8). Hence, $p^2t|L_{npt}$ and the theorem is proved if we have $p \equiv 1 \pmod 4$.

Suppose $p = 4k + 3$. An argument similar to the above yields

$$L_{npt} = L_{nt}\left(\sum_{q=1}^{k+1} L^2_{nt(2k-2q+3)} + \sum_{q=0}^{k-1} (-1)^{n+1}5F^2_{2nt(k-q)} - p(-1)^n\right) \tag{9}$$

and we see, as before, that $p^2t \mid L_{npt}$ if $p \equiv 3 \pmod 4$.

Since $3 \mid L_2$, we have

$$3^k \mid L_{2\cdot 3^{k-1}} \quad \text{or} \quad 3^k \mid L_{2\cdot 3^k} \quad \text{for} \quad k \geq 1 .$$

However, $2 \mid L_{2\cdot 3^k}$ for $k \geq 1$. But $(2,3) = 1$ and we have an alternate proof of Theorem 1 so that Theorem 1 is now an immediate consequence of Theorem 2. Furthermore, this procedure can be used to establish sequences $\{n_k\}$ such that $n_k \mid L_{n_k}$. We have

Theorem 3. Let p be any odd prime different from 3 and such that $p \mid L_{2\cdot 3^k}$, $k \geq 1$. Let $n = 2\cdot 3^k p^t$ where $t \geq 1$; then $n \mid L_n$.

Proof. By Theorem 1 and (3), we see that $2\cdot 3^k \mid L_{2\cdot 3^k p^t}$ for all $t \geq 1$. However, by Theorem 2 and (3), one has $p^t \mid L_{2\cdot 3^k p^t}$ for $t \geq 1$. Since $(2\cdot 3^k, p^t) = 1$, one has $2\cdot 3^k p^t \mid L_{2\cdot 3^k p^t}$ for $t \geq 1$.

By an argument similar to that of Theorem 3, it is easy to see that the following are true.

Corollary 1. If p and q are distinct odd primes such that $p \mid L_n$ and $q \mid L_m$ where m and n are odd, then $(pq)^k \mid L_{mn(pq)^{k-1}}$ for all $k \geq 1$.

and

Corollary 2. If p and q are distinct odd primes different from 3 such that $p \mid L_{2\cdot 3^k}$ and $q \mid L_{2\cdot 3^k}$ where $k \geq 1$ and $n = 2\cdot 3^k p^t q^r$ then $n \mid L_n$ for $t \geq 0$ and $r \geq 0$.

Using $F_{2r} = F_r L_r$, we have

Corollary 3. If p is an odd prime and $p \mid L_n$ then $p^k \mid F_{2np^{k-1}}$ for $k \geq 1$.

and

Corollary 4. If p and q are distinct odd primes such that $p \mid L_n$ and $q \mid L_m$ where m and n are odd integers then $(pq)^k \mid F_{2mn(pq)^{k-1}}$ for $k \geq 1$.

Corollaries 3 and 4 can be strengthened if we know that p is an odd prime and $p \mid F_n$. To do this, we show another theorem discovered independently by Carlitz and Bergum.

Theorem 4. If p is an odd prime and $p \mid F_n$ then $p^k \mid F_{np^{k-1}}$ for all $k \geq 1$.

Proof. By hypothesis, the theorem is true for $k = 1$. Assume $p^k \mid F_{np^{k-1}}$ and let $t = p^{k-1}$ then $pt \mid F_{nt}$. We shall show that $p^2t \mid F_{npt}$. Using Binet's formula together with the factorization of $x^p - y^p$, we have

$$F_{npt} = F_{nt}\sum_{i=1}^{p} \alpha^{nt(p-i)}\beta^{nt(i-1)} . \tag{10}$$

The middle term of the summation is $(-1)^{n(p-1)/2}$ while the sum of the q^{th} and $(p+1-q)^{th}$ terms, where $q \neq (p+1)/2$, using the formula $L_{2r} = 5F_r^2 + 2(-1)^r$, is

$$\alpha^{nt(p-q)}\beta^{nt(q-1)} + \alpha^{nt(q-1)}\beta^{nt(p-q)} = (-1)^{n(q-1)} L_{2nt(p-2q+1)/2} \tag{11}$$

$$= (-1)^{n(q-1)} 5F^2_{nt(p-2q+1)/2} + 2(-1)^{n(p-1)/2} .$$

By substitution into (10), we obtain

$$F_{npt} = F_{nt}\left(\sum_{q=1}^{p-1/2} (-1)^{n(q-1)} 5F^2_{nt(p-2q+1)/2} + p(-1)^{n(p-1)/2}\right) . \tag{12}$$

Using $pt|F_{nt}$ and (1), we see that p is a factor of the expression in the parentheses of (12) so that $p^2t \mid F_{npt}$ and the theorem is proved.

Let $F_n(L_n)$ be the least such that $p|F_n(p|L_n)$ then it is still unresolved if $p^k|F_m(p^k|L_m)$ or $p^k\nmid F_m(p^k\nmid L_m)$ for $np^{k-2} < m < np^{k-1}$ and $k \geq 2$.

An immediate consequence of Theorem 4, by use of (1), is

Corollary 5. If p and q are distinct odd primes such that $p|F_n$ and $q|F_m$ then $(pq)^k|F_{mn(pq)^{k-1}}$ for $k \geq 1$.

Another result of Theorem 4 which was already discovered by Kramer and Hoggatt and occurs in [2] is

$$5^k | F_{5^k}, \quad \text{for} \quad k \geq 1 \tag{13}$$

since $F_5 = 5$. Note that this result also gives us a sequence $\{n_k\}$ such that $n_k|F_{n_k}$.

Just as the authors could find several sequences $\{n_k\}$ such that $n_k|L_{n_k}$ they were also able to show that there are several other sequences $\{n_k\}$ such that $n_k|F_{n_k}$. With this in mind, we prove the next four theorems.

Theorem 5. If $n = 3^m 2^{r+1}$ where $m \geq 1$ and $r \geq 1$ then $n|F_n$.

Proof. By the discussion following Theorem 2 and Corollary 3, we have $3^m|F_{4\cdot 3^m}$ for $m \geq 1$. But $4|F_6$ so that $4|F_{4\cdot 3^m}$ for $m \geq 1$. Since $(4, 3^m) = 1$, we have $4\cdot 3^m|F_{4\cdot 3^m}$ for $m \geq 1$ and the theorem is proved if $r = 1$.

Since

$$F_{3^n 2^{r+2}} = F_{3^m 2^{r+1}} L_{3^m 2^{r+1}} = F_{3^m 2^{r+1}}(5F^2_{3^m 2^r} + 2)$$

and $2|F_3$, we have by induction on r that $3^m 2^{r+2}|F_{3^m 2^{r+2}}$.

Theorem 6. If

$$n = 2^{r+1} 3^m 5^k,$$

where $r \geq 1$, $m \geq 1$, and $k \geq 1$ then $n|F_n$.

Proof. This result follows immediately from Theorem 5, (1), and (13) because

$$(5^k, 2^{r+1}3^m) = 1.$$

By using Theorem 4 and Corollary 5 in an argument similar to that of Theorem 6, we have

Theorem 7. Let p be any odd prime different from 3 and such that $p \mid F_{2^{r+1}3^m}$ where $r \ge 1$ and $m \ge 1$. Let $n = 2^{r+1}3^m p^k$ where $k \ge 1$, then $n \mid F_n$.

and

Theorem 8. Let $s = 2^{r+1}3^m$. Let p and q be distinct odd primes such that $p \mid F_s$ and $q \mid F_s$. Let $n = sp^kq^t$ where $k \ge 0$ and $t \ge 0$ then $n \mid F_n$.

For our next divisibility property, we establish

Theorem 9. If $k \ge 1$ then $2^{k+2} \mid F_{3 \cdot 2^k}$.

Proof. Since $8 \mid F_6$, the theorem is true for $k = 1$. Suppose $s = 2^{k-1}$ and $8s \mid F_{6s}$. Since $F_{12s} = F_{6s}L_{6s} = F_{6s}(5F_{3s}^2 + 2)$ and $2 \mid F_3$, the result follows by induction with the use of (1).

Throughout the remainder of this paper, we analyze the prime decomposition of L_n where n is odd and establish several congruence relations between the elements of $\{F_n\}$ and $\{L_n\}$. With this in mind, we first establish

Lemma 1. If n is odd then $L_n = 4^tM$ where $t = 0$ or 1 and M is odd.

Proof. Since n is odd, we have (1) $L_n = L_{3m+1}$ where m is even, (2) $L_n = L_{3m+2}$ where m is odd, or (3) $L_n = L_{3m}$ where m is odd.

If $L_n = L_{3m+1}$ and $m = 2r$ then $L_n = L_{6r+1}$. Since $2 \mid F_{3r}$, $L_{6r} = 5F_{3r}^2 + 2(-1)^r$, and $(L_{6r}, L_{6r+1}) = 1$, we have L_{3m+1} is odd or that $L_{3m+1} = 4^0M$ where M is odd.

By a similar argument, it is easy to show that $L_{3m+2} = 4^0M$ where M is odd.

Suppose $L_n = L_{3m}$ where $m = 2r + 1$. By an argument similar to that of Theorem 2, it is easy to show that

$$L_n = L_{6r+3} = \begin{cases} 4\left(\sum_{q=0}^{r-1} 5F_{3(r-q)}^2 + 1\right) & \text{if } r \text{ is even;} \\ 4\left(\sum_{q=0}^{r-1} 5F_{3(r-q)}^2 - 1\right) & \text{if } r \text{ is odd .} \end{cases} \tag{14}$$

Now $2 \mid F_{3(r-q)}$ so that the terms in the parentheses are odd and $L_n = 4M$ where M is odd.

The following theorem is due to Hoggatt while the proof is that of Brother Alfred Brousseau.

Theorem 10. The Lucas numbers L_n with n odd have factors 4^tM where $t = 0$ or 1 and the prime factors of M are primes of the form $10m \pm 1$.

Proof. The first part of the theorem is a result of Lemma 1.

From $L_n^2 - L_{n-1}L_{n+1} = (-1)^n 5$, we have that $L_{n-1}L_{n+1} \equiv 5 \pmod p$ for any odd prime divisor p of L_n. However, $L_{n+1} = L_n + L_{n-1}$ so that $L_{n+1} \equiv L_{n-1} \pmod p$.

Therefore, $L_{n-1}^2 \equiv 5 \pmod p$ and 5 is a quadratic residue modulo p. Since the only primes having 5 as a quadratic residue are of the form $10m \pm 1$, we are through.

Using Binet's formula, it can be shown that

$$L_{12t+j} = 5F_{(12t+j-1)/2}F_{(12t+j+1)/2} + (-1)^{(j-1)/2}, \quad j \text{ odd}. \tag{15}$$

Combining the results of Lemma 1 with (15), we have

Theorem 11. There exists an integer N such that

(a) $$L_{12t+1} = 10N + 1,$$

(b) $$L_{12t+3} = 4(10N + 1),$$

(c) $$L_{12t+5} = 10N + 1,$$

(d) $$L_{12t+7} = 10N - 1,$$

(e) $$L_{12t+9} = 4(10N - 1),$$

and

(f) $$L_{12t+11} = 10N - 1.$$

Since the proof of Theorem 11 is trivial, it has been omitted. However, a word of caution about the results is essential. Even though $L_{12t+3} = 4(10N + 1)$ and $L_{12t+5} = 10N + 1$, not all prime factors are of the form $10n + 1$ since $19^2 | L_{12\cdot 14+3}$ and $199^2 | L_{12\cdot 182+5}$. However, the number of prime factors of the form $10n - 1$ which divide L_{12t+3} or L_{12t+5} must be even.

Since $11^2 | L_{4\cdot 12+7}$, $211 | L_{12\cdot 1+9}$ and $11^2 | L_{12\cdot 22+11}$, we see that there can be primes of the form $10n + 1$ which divide L_{12t+j} for $j = 7, 9$, or 11. In fact, the number of primes of the form $10n - 1$ which divide L_{12t+j} where $j = 7, 9$, or 11 must be odd.

Examining [4], we see that $L_{49} = 29 \cdot 599786069$ so that L_{12t+1} may have prime factors of the form $10n \pm 1$.

By Binet's formula, we have

$$F_{n+6} - F_{n-2} = L_n + L_{n+4} = L_{n+2}L_2. \tag{16}$$

Hence, by expanding and substitution of (16), we have

$$\sum_{i=0}^{2^j-1} L_{n+4i} = F_{n+2^{j+2}-2} - F_{n-2}. \tag{17}$$

Using (16) and induction, it can be shown that

$$\sum_{i=0}^{2^j-1} L_{n+4ki} = L_{n+(2^j-1)2k} \prod_{i=1}^{j} L_{2^ik}, \qquad j \geq 1. \tag{18}$$

Hence, by (17) and (18) with $k = 1$ and n replaced by $n + 2$, we have

$$L_{n+2^j+1} \prod_{i=1}^{j} L_{2^i} = F_{n+2^{j+2}} - F_n \tag{19}$$

so that

$$F_{n+2^{j+2}} \equiv F_n \pmod{L_{2^i}} \qquad \text{for} \quad 1 \leq i \leq j \tag{20}$$

and

$$F_{n+2^{j+2}} \equiv F_n \pmod{L_{n+2^j+1}} \quad \text{if} \quad j \neq 0. \tag{21}$$

In papers to follow, the authors will generalize, where possible, the results of this paper to the generalized sequence of Fibonacci numbers as well as to several general linear recurrences. They will also investigate sums and products of the form occurring in (18).

REFERENCES

1. V. E. Hoggatt, Jr., Fibonacci and Lucas Numbers, Houghton Mifflin Co., 1969.
2. Judy Kramer and V. E. Hoggatt, Jr., "Special Cases for Fibonacci Periodicity," Fibonacci Quarterly, Vol. 10, No. 5, pp. 519-522.
3. I. Niven and H. Zuckerman, An Introduction to the Theory of Numbers, John Wiley and Sons, Inc., 1960.
4. Fibonacci and Related Number Theoretical Tables, edited by Brother Alfred Brousseau, Fibonacci Association, 1972, p. 11.
5. Larry Lang, Fibonacci Quarterly, Elementary Problem No. B-247, Vol. 10, No. 5 (Dec. 1972).