ON THE FACTORIZATION OF LUCAS NUMBERS

Wayne L. McDaniel
University of Missouri-St. Louis, MO 63121
(*Submitted March 1999*)

1. INTRODUCTION

If an integer is not a prime, then it can, of course, be written as the product of two integers, say r and $r+k$. In the case of the Lucas numbers, L_n, it has been shown that the two factors may differ by 0 (that is, L_n is a square) only if $n=1$ or 3 [1], [3], may differ by 1 only if $n=0$ [4], [5], and may differ by 2 only if $n=\pm 2$ [6].

It is well known that $L_n^2-5F_n^2=4(-1)^n$, where F_n is the n^{th} Fibonacci number, so if $L_n = r(r+k)$, we have an equation of the form $x^4+2kx^3+x^2k^2\pm 4=5y^2$. Since the left side has 3 distinct zeros, the number of solutions of this equation is finite, by a theorem of Siegel [7]; further, by a theorem of Baker (see [2]), $|x|$ and $|y|$ are effectively bounded. Hence, for a given k, the number of integers n such that $L_n=r(r+k)$ is finite, but the known bounds are extremely large.

We shall show that, if $L_n=r(r+k)$ for $k\equiv 1,6,7,8,17,18,19$, or 24 (mod 25), the number of solutions is bounded by one-half the number of positive divisors of $|k^2-8|$ or $|k^2+8|$, and we provide an algorithm for finding all solutions. In each case,

$$n<\frac{2\log((k^2+9)/4)}{\log((1+\sqrt{5})/2)}.$$

For certain infinite sets, e.g., $k\equiv 8$ (mod 100), we show that no solutions exist. When k is even, $L_n=r(r+k)$ is equivalent to $L_n=x^2-(k/2)^2$, so our results extend Robbins' result [6] on the solutions of $L_n=x^2-1$ to the difference of two squares in infinitely many cases.

We write $\square$ for "a square," τ is the usual "number of divisors" function, $(a\,|\,b)$ is the Jacobi symbol, and we will need the following familiar relations. Let g, m, n, and t be integers, t odd.

$$L_{2g}=L_g^2-2(-1)^g \quad\text{and}\quad F_{2g}=F_gL_g, \tag{1}$$

$$L_{-n}=(-1)^nL_n \quad\text{and}\quad F_{-n}=(-1)^{n+1}F_n, \tag{2}$$

$$2L_{m+n}=L_mL_n+5F_mF_n, \tag{3}$$

$$L_{2^um}\equiv\begin{cases}2 \pmod 8 & \text{if } 3\,|\,m \text{ and } u\ge 1,\\ -1 \pmod 8 & \text{if } 3\nmid m \text{ and } u\ge 2,\end{cases} \tag{4}$$

$$L_{2gt+m}\equiv \pm L_{2g+m} \pmod{L_{2g}}. \tag{5}$$

2. L_n AS THE PRODUCT OF TWO FACTORS DIFFERING BY k

We assume, without loss of generality, that k is positive, and note that $L_n=r(r+k)$ for some r implies that $4L_n+k^2=\square$.

Lemma 1: Let $L_n=r(r+k)$. If $k\equiv\pm 11$ (mod $3\cdot 25\cdot 41$), then $n\equiv 0$ (mod 4).

Proof: Let $k = \pm 11 \pmod{3\cdot 25\cdot 41}$. We find that $4L_n + k^2$ is a quadratic residue modulo 25 only for $n \equiv 0, 1, 4, 8, 9, 12,$ or $16 \pmod{20}$; if n is odd, then $n \equiv 1, 9, 21,$ or $29 \pmod{40}$. Now, the Lucas numbers are periodic modulo 41 with period of length 40, and $4L_n + k^2$ is a quadratic nonresidue modulo 41 for $n \equiv 9, 21,$ and $29 \pmod{40}$, and is a quadratic nonresidue modulo 3 for $n \equiv 1 \pmod 8$. It follows that $4L_n + k^2 = \Box$ only if $n \equiv 0, 4, 8, 12,$ or $16 \pmod{20}$; that is, only if $n \equiv 0 \pmod 4$.

Let

$$S_1 = \{k \mid k \equiv 1, 6, 19, \text{ or } 24 \pmod{25}\},$$
$$S_2 = \{k \mid k \equiv 7, 8, 17, \text{ or } 18 \pmod{25}\},$$

and

$$S_3 = \{k \mid k \equiv \pm 11 \pmod{3\cdot 25\cdot 41}\}.$$

Theorem 1: Let $k \in S_1 \cup S_2 \cup S_3$. The number of nonnegative integers n for which $L_n = r(r+k)$ is less than or equal to $\tau(k^2-8)/2$ if $k \in S_1 \cup S_3$, and less than or equal to $\tau(k^2+8)/2$ if $k \in S_2$. If $L_n = r(r+k)$, then

$$n < \frac{2\log((k^2+9)/4)}{\log((1+\sqrt{5})/2)}.$$

Proof: Assume that $L_n = r(r+k)$; then $4L_n + k^2 = \Box$. The quadratic residues modulo 25 are the integers in $T = \{0, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24\}$.

We find that, for each integer k in S_1, $4L_n + k^2 \equiv$ an element of $T \pmod{25}$, precisely when $n \equiv 0, 4, 8, 12,$ or $16 \pmod{20}$; combining this with the result of Lemma 1, we have $L_n = r(r+k)$ for each integer k in $S_1 \cup S_2$ only when $n \equiv 0 \pmod 4$. And, for each integer k in S_2, $4L_n + k^2 \equiv$ an element of $T \pmod{25}$, precisely when $n \equiv 2, 6, 10, 14,$ or $18 \pmod{20}$, i.e., only when $n \equiv 2 \pmod 4$.

Let $n = 2t$. Now, $L_n = r(r+k)$ implies that there exists an x such that $x^2 = 4L_{2t} + k^2$, so, by (1), we have $x^2 - (2L_t)^2 = k^2 - 8(-1)^t$. Hence, there exist divisors c and d of $k^2 - 8(-1)^t$ such that $x + 2L_t = c$ and $x - 2L_t = d$, implying that $L_t = \frac{c-d}{4}$. Since, for a given pair (c, d) of divisors of $k^2 - 8(-1)^t$, the system has at most one solution; there exist at most $\tau[k^2 - 8(-1)^t]/2$ integers n for which $L_n = r(r+k)$. Taking t even or odd for the two cases, respectively, proves the first statement of the theorem.

It is well known that $L_n = \alpha^n + \beta^n$, where $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$. Let $s = [k^2 - 8(-1)^t - 1]/4$. Since $\alpha^t - 1/\alpha^t = \alpha^t + \beta^t = L_t = \frac{c-d}{4} \le s$, we readily obtain $\alpha^t < (s + \sqrt{s^2+4})/2$ If $k = 1$, it is easily seen that $n = 0$, and if $k \neq 1$, then $\alpha^t < [s + (s+1)]/2$. One obtains a relatively simple bound upon taking the logarithm of each side of $\alpha^t < s + \frac{1}{2}$, replacing t by $n/2$ and replacing s by the larger of its two values.

Lemma 2: If $k \equiv 0 \pmod 4$, then $L_n = r(r+k)$ only if n is odd.

Proof: Let $k = 4t$, and assume that, for some m, $L_{2m} = r(r+k)$. Then

$$L_{2m} + 4t^2 = r^2 + 4rt + 4t^2 = \Box,$$

implying $L_{2m} \equiv 0$ or $1 \pmod 4$, contrary to (4).

We now exhibit several infinite sets of integers k such that L_n does not have the form $r(r+k)$ for any n.

Theorem 2: Let $S = \{k \mid k \equiv 8, 24, 32, 44, 56, 68, 76, 92 \pmod{100}\}$. If $k \in S$, then $L_n \neq r(r+k)$ for any n.

Proof: Let $k \in S$ and assume, for some $n \geq 0$ and some integer r, that $L_n = r(r+k)$. By Lemma 2, n is odd. However, each element of S is in $S_1 \cup S_2$ and, as noted in the proof of Theorem 1, $4L_n + k^2$ is a quadratic nonresidue for n odd.

Corollary: There exist infinitely many primes p such that L_n does not have the form $r(r+4p)$ for any n.

Proof: The sequence $\{2+25b\}$ contains infinitely many primes p and, for $p = 2+25b$, we have $4p \equiv 8 \pmod{100}$.

3. L_n AS THE DIFFERENCE OF TWO SQUARES

The proof of the following theorem is immediate upon writing $x^2 - m^2$ as $r(r+k)$ with $r = x - m$ and $k = 2m$.

Theorem 3: The equation $L_n = x^2 - m^2$

a) is impossible for all $n \geq 0$ if $m \equiv 4, 12, 16, 22, 28, 34, 38,$ or $46 \pmod{50}$,

b) has at most $\tau(4m^2 - 8)/2$ solutions if $2m \in S_1$, and

c) has at most $\tau(4m^2 + 8)/2$ solutions if $2m \in S_2 \cup S_3$,

and, if $L_n = x^2 - m^2$, then

$$n < \frac{2\log(m^2 + 9/4)}{\log((1+\sqrt{5})/2)}.$$

In practice, for a given m, one may find the values of n such that $L_n = x^2 - m^2$ by proceeding as in the proof of Theorem 1: simply write $L_{n/2} = \frac{c-d}{4}$ for all pairs (c, d), $c \equiv d \pmod 4$, of factors of $|4m^2 - 8(-1)^{n/2}|$, and find n. We can now readily obtain the values of n for which $L_n = x^2 - m^2$ for all m such that $2m = k \in S_1 \cup S_2 \cup S_3$. Notice that L_{-n} is the difference of two squares iff L_n is the difference of two squares, since $L_{-n} = \pm L_n$.

By way of example, if $m = 3$, then $2m = 6 \in S_1$, $4m^2 - 8(-1)^{n/2} = 28$, and $L_{n/2} = \frac{c-d}{4}$ for $(c, d) = (14, 2)$; hence, $L_{n/2} = 3$, and we conclude that $L_n = x^2 - 3^2$ only when $n = \pm 4$ ($L_{\pm 4} = 7 = 4^2 - 3^2$).

It may be noted that we now know the values of n for which $L_n = x^2 - m^2$ for $m = 1, 3,$ and 4, and can determine the n for many larger values of m. In order to close the gap between 1 and 3, we shall prove that $L_n \neq x^2 - 2^2$ for any n. Unlike the cases considered above, this case presents a difficulty that precludes the possibility of establishing a bound on n for all $k \equiv 2m \equiv 4 \pmod M$ for any M.

Lemma 3: If $3 \nmid g$, then $L_{2g \pm 3} \equiv 5F_{2g} \pmod{L_{2g}}$.

Proof: We note first that $F_{\pm 3} = 2$. By (3),

$$2L_{2g\pm 3} = L_{2g}L_{\pm 3} + 5F_{2g}F_{\pm 3} \equiv 10F_{2g} \pmod{L_{2g}}.$$

Since $3 \nmid g$, L_{2g} is odd, and the lemma follows.

Lemma 4: If $3 \nmid g$ and t is odd, then $(L_{2gt\pm 3} + 4 \mid L_{2g}) = (5F_{2g} + 4 \mid L_{2g})$.

Proof: By (5) and Lemma 3,

$$(L_{2gt\pm 3} + 4 \mid L_{2g}) = (\pm L_{2g\pm 3} + 4 \mid L_{2g}) = (5F_{2g} + 4 \mid L_{2g}) \text{ or } (-5F_{2g} + 4 \mid L_{2g}).$$

We prove that these latter two Jacobi symbols are equal by showing that their product is +1:

$$\begin{aligned}(5F_{2g} + 4 \mid L_{2g}) \cdot (-5F_{2g} + 4 \mid L_{2g}) &= (16 - 25F_{2g}^2 \mid L_{2g}) \\ &= (16 - 5(L_{2g}^2 - 4) \mid L_{2g}) = (36 \mid L_{2g}) = +1.\end{aligned}$$

Lemma 5: Let $u \geq 4$. Then $5F_{2^u m} + 2L_{2^u m} \equiv -1 \pmod 8$ $\begin{cases}\text{if } u \text{ is odd and } m = 1, \text{ or} \\ \text{if } u \text{ is even and } m = 5.\end{cases}$

Proof: Let $m > 0$. By (1) and (4),

$$F_{2^u m} = F_{2^{u-2}m}L_{2^{u-2}m}L_{2^{u-1}m} \equiv F_{2^{u-2}m} \equiv F_{2^{u-4}m} \equiv \cdots F_{4m} \text{ or } F_{8m} \pmod 8,$$

depending on whether u is even or odd, respectively. Using (4), $F_8 = 21$, and $F_{20} = 6765$ proves the lemma.

Theorem 4: No term of the sequence $\{L_n\}$ is of the form $x^2 - 4$.

Proof: Assume $L_n = x^2 - 4$. By Lemma 2, we may assume that n is odd. Now $\square = L_n + 4$ modulo 25 only if $n \equiv 13$ or 17 (mod 20), and modulo 11 only if $n \equiv 5, 7, 9$ (mod 10). It follows that $n \equiv 1$ (mod 4) and $n \equiv -3$ (mod 5). For $n \equiv 1$ (mod 4), $\square = L_n + 4$ modulo 7 and modulo 47 only if $n \equiv -3$ or 13 (mod 32). However $L_n + 4$ has period of length 64 modulo 2207, and 13 and 45 are quadratic nonresidues modulo 64; hence, $n \equiv -3$ (mod 32). Combining this with $n \equiv -3$ (mod 5), we have $n \equiv -3$ (mod $5 \cdot 32$).

Let $n = 2gt - 3$, with t odd, $g = 2^u$ if u is odd, and $g = 2^u \cdot 5$ if u is even ($u \geq 4$). We shall use (1), (4), Lemma 5, and the following observation:

$$2L_{2g} = 2(L_g^2 - 2) = 2L_g^2 + 5L_g^2 - L_g^2 = 5F_g^2 + L_g^2. \tag{6}$$

By Lemma 4,

$$\begin{aligned}(L_n + 4 \mid L_{2g}) &= (5F_{2g} + 4 \mid L_{2g}) = (5F_{2g} + 2(L_g^2 - L_{2g}) \mid L_{2g}) = (5F_{2g} + 2L_g^2 \mid L_{2g}) \\ &= (L_g \mid L_{2g})(5F_g + 2L_g \mid L_{2g}) = -(L_{2g} \mid L_g)(-1)(L_{2g} \mid 5F_g + 2L_g) \\ &= (L_g^2 - 2 \mid L_g)(2 \mid 5F_g + 2L_g)(2L_{2g} \mid 5F_g + 2L_g) \\ &= (-1 \mid L_g)(5F_g^2 + L_g^2 \mid 5F_g + 2L_g) \qquad \text{[by (6)]} \\ &= -(45F_g^2 - (25F_g^2 - 4L_g^2) \mid 5F_g + 2L_g) = -(5 \mid 5F_g + 2L_g) \\ &= -(5F_g + 2L_g \mid 5) = -(2 \mid 5)(L_g \mid 5) = (L_g \mid 5).\end{aligned}$$

Since $L_8 = 47 \equiv 2 \pmod 5$, by (1), $L_{16} \equiv 2 \pmod 5$, and, by induction, $L_{2^u} \equiv 2 \pmod 5$. Similarly, $L_{20} = 15127 \equiv 2 \pmod 5$, implying $L_{2^u \cdot 5} \equiv 2 \pmod 5$. Hence, $(L_g \mid 5) = (2 \mid 5) = -1$, a contradiction.

ACKNOWLEDGMENT

The idea for this article occurred to the author following receipt by e-mail from Richard André-Jeannin of a much shorter proof of a theorem in my article "Pronic Lucas Numbers" [5]. André-Jeannin's proof did not involve congruences moduli L_{2g}, where g is a function of n, and the absence of such congruences is essential to obtaining the above results. It is the necessity of over-coming this obstacle that suggests that obtaining an analogous result for the Fibonacci numbers may be difficult.

REFERENCES

1. Brother U. Alfred. "On Square Lucas Numbers." *The Fibonacci Quarterly* **2.1** (1964):11-12.
2. A. Baker. *Transcendental Number Theory*. Cambridge: Cambridge University Press, 1975.
3. J. H. E. Cohn. "Square Fibonacci Numbers, Etc." *The Fibonacci Quarterly* **2.2** (1964):109-113.
4. Ming Luo. "Nearly Square Numbers in the Fibonacci and Lucas Sequences." *Journal of Chongqing Teacher's College* **12.4** (1995):1-5. (In Chinese.)
5. Wayne L. McDaniel. "Pronic Lucas Numbers." *The Fibonacci Quarterly* **36.1** (1998):60-62.
6. N. Robbins. "Fibonacci and Lucas Numbers of the Forms $w^2 - 1$, $w^3 \pm 1$." *The Fibonacci Quarterly* **19.4** (1981):369-73.
7. C. L. Siegel. "Über einige Anwendungen diophantischer Approximationen" (1929), pp. 209-266. In *Collected Works*. New York: Springer-Verlag, 1966.

AMS Classification Numbers: 11B39

❖❖❖