Internat. J. Math. & Math. Sci.
VOL. 14 NO. 4 (1991) 697-704

LUCAS NUMBERS OF THE FORM PX^2, WHERE P IS PRIME

NEVILLE ROBBINS

Mathematics Dept.
San Francisco State University
San Francisco, CA 94132 USA

(Received February 1, 1989 and in revised form February 8, 1990)

ABSTRACT. Let L_n denote the n^{th} Lucas number, where n is a natural number. Using elementary techniques, we find all solutions of the equation: $L_n = px^2$ where p is prime and $p < 1000$.

KEY WORDS AND PHRASES. Lucas number
1985 AMS SUBJECT CLASSIFICATION CODE. 11B39

1. INTRODUCTION

Let n denote a natural number. Let L_n denote the n^{th} Lucas number, that is, $L_1=1$, $L_2=3$, $L_n = L_{n-1}+L_{n-2}$ for $n \geq 3$. In [1], J.H.E. Cohn found all Lucas numbers which are square or twice a square. As a result of a later paper of Cohn [2], it is known that for each integer $c \geq 3$, there is at most one Lucas number of the form cx^2. Using [3], Definition 2, and (9) below, we see that there are 111 primes, p, such that (i) $2 < p < 1000$, and (ii) there exists n such that $p|L_n$. In this paper, we find all solutions of the equation:

$$L_n = px^2 \tag{*}$$

where the prime p satisfies conditions (i) and (ii) above. We find that only 8 such values of p yield solutions of (*). The results are summarized in Table 3 on the last page. The larger problem of finding all solutions to (*) appears more difficult; its solution would yield all Lucas numbers which are prime.

2. PRELIMINARIES

Let n denote a natural number. Let p denote a prime, not necessarily satisfying conditions (i) and (ii) above.

Definition 1 Let F_n denote the n^{th} Fibonacci number, that is, $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$.

Definition 2 Let $z(n) = \text{Min}\{k: k \geq 1 \text{ and } n|F_k\}$.

Definition 3 Let $y(n) = \frac{1}{2}z(n)$ if $2|z(n)$.

For each integer $c \geq 3$, the equation $L_n = cx^2$ has at most one solution. (1)

If $L_n=q$ is prime, then $y(q)=n$ and $y(q^2)=qn$. (2)

$(L_n, L_{3n}/L_n) = \begin{cases} 3 \text{ if } n \equiv 2 \pmod 4 \\ 1 \text{ otherwise} \end{cases}$ (3)

$L_n = x^2$ iff n=1 or 3 (4)

$L_{3n} = L_n(L_n^2 - 3(-1)^n)$ (5)

If m is odd and $m \geq 3$, then $m|L_n$ iff $\frac{n}{y(m)}$ is an odd integer (6)

$(L_n, L_{5n}/L_n) = 1$ (7)

If k is odd, then $(L_n, L_{kn}/L_n)|k$. (8)

If p is an odd prime, then $p|L_n$ iff $\frac{2n}{z(p)}$ is an odd integer. (9)

$L_{2n} = L_n^2 - 2(-1)^n$ (10)

$L_n|L_{kn}$ iff k is odd or n=1. (11)

$L_{mn}/L_n = (-1)^{\frac{1}{2}(m-1)(n+1)} + \sum_{j=1}^{\frac{1}{2}(m-1)} (-1)^{(j-1)(n+1)} L_{(m+1-2j)n}$ if m is odd. (12)

If p is odd and $p|L_n$, then $2 \leq y(p) \leq \frac{1}{2}(p+1)$. (13)

If p and m are odd, $p \nmid m$, and $p^h || L_n$, then $p^{h+k} || L_{mnp^k}$ for all $k \geq 0$. (14)

$L_{2^n} \equiv 3 \pmod 4$ for all $n \geq 1$. (15)

$L_{8n} \equiv 2 \pmod 3$ for all $n \geq 1$. (16)

If p is a prime such that y(p) exists, then (p,y(p)) = 1. (17)

If m/(m,n) and n/(m,n) are both odd, then $(L_m, L_n) = L_{(m,n)}$ (18)

If $y(p^2) = py(p)$, then $y(p^k) = p^{k-1}y(p)$ for all $k \geq 1$. (19)

Remarks: (1) follows from Theorem 11 in [2] with a=1; (4) is Theorem 1 in [1]; (8) follows from Theorem 4 in [5]; (12) follows from (44) in [4]; (14) follows from Theorem XI in [6]; (19) follows from (14). The other identities are elementary.

3. THE MAIN RESULTS

THEOREM 1 If p is a prime such that y(p) exists and $L_{y(p)} = pu^2$, then (*) has the unique solution: n = y(p), $x^2 = u^2$.

PROOF: This follows from hypothesis and (1).

THEOREM 2 If $p \in \{3,7,11,19,29,47,199,521,2207,9349\}$, then (*) has a solution with n = 2,4,5,9,7,8,11,13,16,19 respectively; if p=19, then $x^2=4$; in each other case, $x^2=1$.

PROOF: This follows from (2) and Theorem 1, since $L_2=3$, $L_4=7$, $L_5=11$, $L_9=19*4$, $L_7=29$, $L_8=47$, $L_{11}=199$, $L_{13}=521$, $L_{16}=2207$, $L_{19}=9349$, and y(19)=9.

THEOREM 3 $L_{3k} = px^2$ iff either (i) k=p=2, $x^2=9$, or (ii) k=3, p=19, $x^2=4$.

PROOF: Sufficiency is readily shown, since $L_6=18=2(3)^2$ and $L_9=76=19(2)^2$. Now suppose $L_{3k} = px^2$. Let $d = (L_k, L_{3k}/L_k)$. If $k \not\equiv 2 \pmod 4$, then (3) implies d=1, so (1) implies $L_k=u^2$, $L_{3k}/L_k = pv^2$ for some u,v. Now (4) implies k=1 or 3. If k=1, then $L_3/L_1 = 4 = pv^2$, an impossibility. If k=3, then $L_9/L_3 = 19 = pv^2$, so p=19 and $x^2 = L_9/19 = 4$. If $k \equiv 2 \pmod 4$, then (3) implies d=3, so either (i) $L_k = 3u^2$, $L_{3k}/L_k = 3pv^2$, or (ii) $L_k = 3pu^2$, $L_{3k}/L_k = 3v^2$ for some u,v. If (i) holds, then Theorem 2 implies k=2, so $L_{3k} = L_6 = 18 = px^2$, which implies p=2 and x^2=9. If (ii) holds, then (5) implies $L_{3k}^2-3 = 3v^2$. Since $3|L_k$, we get $3v^2 \equiv -3 \pmod 9$, so $v^2 \equiv -1 \pmod 3$, an impossibility.

THEOREM 4 If $p > 19$ and $3|y(p)$, then $L_n = px^2$ is impossible.

PROOF: If $L_n = px^2$, then $p|L_n$, so (6) implies $y(p)|n$. Now hypothesis implies $3|n$, so n=3k for some k. The conclusion now follows from hypothesis and Theorem 3.

THEOREM 5 (*) has no solution if $p \in \{23,31,79,83,107,167,181,211,227,229, 241,271,349,379,383,409,431,439,443,467,499,503,541,571,587,601,631,647,683,691, 739,751,769,811,827,859,863,887,919,947,983,991\}$.

PROOF: This follows from hypothesis and Theorem 4, since in each case, $p > 19$ and according to [3], $3|y(p)$.

THEOREM 6 $L_{5k} = px^2$ iff $k = x^2 = 1$ and p=11.

PROOF: Sufficiency is readily shown, since $L_5 = 11 = 11*1^2$. Now suppose $L_{5k} = px^2$. Theorem 2 of [1] implies p is odd. Now (7), (1) and hypothesis imply $L_k = u^2$, $L_{5k}/L_k = pv^2$ for some u,v. Now (4) implies k=1 or 3. If k=1, then $pv^2 = L_5/L_1 = 11$, so p=11 and $x^2 = L_5/11 = 1$. If k=3, then $pv^2 = L_{15}/L_3 = 1364/4 = 341 = 11*31$, an impossibility.

THEOREM 7 If $L_n = px^2$ and $5|y(p)$, then n=5, p=11, x^2=1.

PROOF: Hypothesis and (6) imply $y(p)|n$. Therefore hypothesis implies $5|n$, that is, n=5k for some k, so the conclusion follows from Theorem 6.

THEOREM 8 (*) has no solution if $p \in \{41,71,101,131,151,191,251,311,331, 401,491,641,911,941,971\}$.

PROOF: This follows from Theorem 7, since in each case, $p > 11$, and according to [3], $5|y(p)$.

THEOREM 9 Let p be an odd prime such that y(p) exists and is odd, and such that for every prime divisor, q, of y(p), $z(q) \not\equiv 2 \pmod 4$. If $L_n = px^2$, then n = y(p).

PROOF: If $L_n = px^2$, then (6) implies n = my(p) for odd m. Now (8) implies $d|\frac{n}{m}$, that is, $d|y(p)$. If $d > 1$, then there exists an odd prime, q, such that $q|d$. Therefore $q|L_m$, so (9) implies $\frac{2m}{z(q)}$ is an odd integer; since m is odd, this implies $z(q) \equiv 2 \pmod 4$, contrary to hypothesis. Therefore d=1. Now (13) implies $y(p) > 1$, so $m < n$. Therefore hypothesis and (1) imply $L_m = u^2$, $L_n/L_m = pv^2$ for some u,v. Now (4) implies m=1 or 3. If m=3, then $L_n = p(2v)^2$, so Theorem 3 implies n=9, p=19. But then $\frac{n}{y(p)} = 1 \neq 3$. Therefore m=1 so n = y(p).

THEOREM 10 (*) has no solution if $p \in \{139,179,239,461,509,599,619,659\}$.

PROOF: This follows from hypothesis and Theorem 9, since in each case, according to [3] and [7], p fulfills the hypothesis of Theorem 9, yet $L_{y(p)} \neq px^2$.

In the work which follows, we will need the following lemmas:

LEMMA 1 $L_{2^j t} \equiv \begin{cases} 2(-1)^{t+1} & (\text{mod } L_t^2) \text{ if } j=1 \\ 2 & (\text{mod } L_t^2) \text{ if } j \geq 2 \end{cases}$

PROOF: (Induction on j) (10) implies Lemma 1 holds for j=1. If $j \geq 2$, then (10) implies $L_{2^j t} = L^2_{2^{j-1}t} - 2(-1)^{2^{j-1}} = L^2_{2^{j-1}t} - 2$. But $L^2_{2^{j-1}t} \equiv 4 \pmod{L_t^2}$ by induction hypothesis. Therefore $L_{2^j t} \equiv 4-2 \equiv 2 \pmod{L_t^2}$.

LEMMA 2 If $k \geq 1$ and $2|n$, then $L_{2kn} \equiv 2(-1)^k \pmod{L_n^2}$.

PROOF: Hypothesis and (10) imply $L_{2kn} = L_{kn}^2 - 2$. If k is odd, then (11) implies $L_n^2 | L_{kn}^2$, so $L_{2kn} \equiv -2 \equiv 2(-1)^k \pmod{L_n^2}$. If $k = 2^j r$ with $j \geq 1$ and r odd, then Lemma 1 implies $L_{2kn} = L_{2^{j+1} rn} \equiv 2 \pmod{L_{rn}^2}$. Now (11) implies $L_n^2 | L_{rn}^2$, so $L_{2kn} \equiv 2 \equiv 2(-1)^k \pmod{L_n^2}$.

LEMMA 3 If $m-1 \equiv n \equiv 0 \pmod 2$, then $L_{mn}/L_n \equiv m(-1)^{\frac{1}{2}(m-1)} \pmod{L_n^2}$.

PROOF: Hypothesis and (12) imply $L_{mn}/L_n =$ $(-1)^{\frac{1}{2}(m-1)} + \sum_{j=1}^{\frac{1}{2}(m-1)} (-1)^{j-1} L_{(m+1-2j)n}$. Hypothesis and Lemma 2 imply $L_{(m+1-2j)n} \equiv 2(-1)^{\frac{1}{2}(m+1-2j)} \pmod{L_n^2}$. Therefore $L_{mn}/L_n \equiv$ $(-1)^{\frac{1}{2}(m-1)} + \sum_{j=1}^{\frac{1}{2}(m-1)} 2(-1)^{\frac{1}{2}(m-1)} \equiv (1+2(\frac{m-1}{2}))(-1)^{\frac{1}{2}(m-1)} \equiv m(-1)^{\frac{1}{2}(m-1)} \pmod{L_n^2}$.

LEMMA 4 If p is an odd prime, $p|L_n$, and $2|n$, then $L_{pn}/pL_n \equiv (-1)^{\frac{1}{2}(p-1)} \pmod p$.

PROOF: Hypothesis and Lemma 3 imply $L_{pn}/L_n \equiv p(-1)^{\frac{1}{2}(p-1)} \pmod{L_n^2}$. Now hypothesis implies $L_{pn}/L_n \equiv p(-1)^{\frac{1}{2}(p-1)} \pmod{p^2}$, from which the conclusion immediately follows.

LEMMA 5 If $2|n$, $p|L_n$, p is prime, and $p \equiv 3 \pmod 4$, then $L_{pn}/pL_n \neq s^2$.

PROOF: Hypothesis and Lemma 4 imply $L_{pn}/pL_n \equiv -1 \pmod p$. Also, hypothesis implies $s^2 \not\equiv -1 \pmod p$, so $L_{pn}/pL_n \neq s^2$.

LEMMA 6 Let $L_n = px^2$ where p and y(p) are odd. Let $m | \frac{n}{y(p)}$. Let $d = (L_m, L_n/L_m)$. Then d=1 iff m=1.

PROOF: If m=1, then $d|L_1$, that is $d|1$, so d=1. Conversely, if d=1, then since hypothesis and (13) imply $m < n$, hypothesis and (1) imply $L_m = u^2$, $L_n/L_m = pv^2$ for some u,v. Now (4) implies m=1 or 3. If m=3, then hypothesis and Theorem 3 imply p=19, n=9=y(19), so $m|1$, an impossibility. Therefore m=1.

LEMMA 7 If $L_n = px^2$, p and y(p) are odd, $m > 1$ and $m \mid \frac{n}{y(p)}$, then $(L_m, L_n/L_m) > 1$.

PROOF: This follows from hypothesis and Lemma 6.

LEMMA 8 Let p, q be odd primes such that $pq \mid L_n$ for some n. Then $2^h \| y(p)$ iff $2^h \| y(q)$, where $h \geq 0$.

PROOF: Hypothesis and (6) imply $n = jy(p) = ky(q)$ with j, k odd. The conclusion now follows.

THEOREM 11 Let $L_n = px^2$, where p is an odd prime, $2^h \| y(p)$ for some $h \geq 1$, and $L_{2^h} = q$ is prime. Then either (i) $n=2^h$, $p=q$, $x^2=1$, or (ii) $n=2^h q$, $p = L_{2^h q}/(qt)^2$, $x^2 = (qt)^2$ for some $t \geq 1$.

PROOF: Hypothesis and (15) imply $q \equiv 3 \pmod 4$, so q is odd. Hypothesis implies $y(p)/2^h$ is odd, so (11) implies $L_{2^h} \mid L_{y(p)}$, that is, $q \mid L_{y(p)}$. Hypothesis and (6) imply $n/y(p)$ is an odd integer, so (11) implies $L_{y(p)} \mid L_n$, hence $q \mid L_n$. If $p=q$, then hypothesis and (1) imply $n=2^h$, $x^2=1$. If $p \neq q$, then hypothesis implies $q \mid x^2$, so $q^2 \mid x^2$, so $q^2 \mid L_n$. Now (6) implies $n = my(q^2)$ for odd m. Hypothesis and (2) imply $y(q^2) = qy(q)$, so $n = mqy(q)$. We have $L_{my(q)}(L_{mqy(q)}/L_{my(q)}) = px^2$. Let $d = (L_{my(q)}, L_{mqy(q)}/L_{my(q)})$. Now (8) implies $d \mid q$; (6) implies $q \mid L_{my(q)}$. Let $q^j \| L_{my(q)}$. Then (14) implies $q^{j+1} \| L_{mqy(q)}$ so $q \| (L_{mqy(q)}/L_{my(q)})$. Therefore $q \mid d$, so $d=q$. Letting $t = x/q$, we obtain $(L_{my(q)}/q)(L_{mqy(q)}/qL_{my(q)}) = pt^2$, where the factors on the left side of the equation are relatively prime. Therefore either (a) $L_{my(q)}/q = pu^2$, $L_{mqy(q)}/qL_{my(q)} = v^2$, or (b) $L_{my(q)}/q = u^2$, $L_{mqy(q)}/qL_{my(q)} = pv^2$ for some u,v. Now hypothesis and (2) imply $y(q) = 2^h$, so Lemma 5 implies (a) is impossible. Therefore (b) must hold. Now (1), (2) and hypothesis imply $m = u^2 = 1$, $L_{qy(q)} = p(qv)^2 = p(qt)^2$, $n = qy(q) = 2^h q$, $x=qt$.

THEOREM 12 If p is an odd prime and $2^h \| y(p)$ where $1 \leq h \leq 4$, then the only solutions of (*) are given by Table 1 below.

Table 1

n	p	x^2
2	3	1
4	7	1
8	47	1
16	2207	1
28	14503	49

PROOF: This follows from hypothesis and Theorem 11, since $L_2=3$, $L_4=7$, $L_8=47$, $L_{16}=2207$ (all primes); also $L_{28} = 14503*7^2$. Note that $L_6/2^2 = 2$ (prime but not odd.) According to [7], $L_{376}/47^2 \neq pt^2$. According to the referee, $1553729 \| L_{35312}$ and $L_{35312}/1553729*2207^2 \neq t^2$.

THEOREM 13 (*) has no solution if $p \in \{43,67,103,163,223,263,281,283,307,347,367,449,463,487,523,547,563,569,607,643,727,743,787,823,881,883,907,929,967\}$.

PROOF: This follows from hypothesis and Theorem 12, since in each case, according to [3], p satisfies the hypothesis of Theorem 12 but does not appear in Table 1 above.

THEOREM 14 $L_{11k} = px^2$ iff $k = x^2 = 1$ and p=199.

PROOF: Sufficiency is readily shown, since $L_{11} = 199 = 199*1^2$. Now suppose $L_{11k} = px^2$. Let $d = (L_k, L_{11k}/L_k)$. (8) implies $d|11$. If d=11, then since y(11)=5, (6) implies $5|k$, so $5|11k$. But then hypothesis and Theorem 6 imply 11k=5, an impossibility. If d=1, then (10) implies $L_k=u^2$, $L_{11k}/L_k = pv^2$ for some u,v. Now (4) implies k=1 or 3. Theorem 3 implies $k \neq 3$, so k=1, hence p=199, $x^2=1$.

THEOREM 15 If $L_n = px^2$ and $11|y(p)$, then n=11, p=199, $x^2=1$.

PROOF: Hypothesis and (6) imply $11|n$, so the conclusion follows from Theorem 14.

THEOREM 16 $L_n = 419x^2$ is impossible.

PROOF: According to [3], y(419) = 209 = 11*19. The conclusion now follows from Theorem 15.

THEOREM 17 $L_n = 127x^2$ is impossible.

PROOF: Suppose $L_n = 127x^2$. Since y(127)=64, (6) implies $64|n$. Hypothesis and (16) now imply $x^2 \equiv 2 \pmod 3$, an impossibility.

THEOREM 18 If p and y(p)=q are primes, $q > 3$, $q^2 \nmid L_{y(q)}$, $p^2 \nmid L_q$, $L_q \neq ps^2$, and either (I) $2|y(q)$ or (II) $2 \nmid y(q)$ and the equation $L_m = qs^2$ (considered as an equation in m) either (A) has no solution or (B) has the solution m=y(q) but there exists a prime, t, such that $t || (L_q/p)$ and $t \nmid y(q)$, then $L_n = px^2$ is impossible.

PROOF: Suppose $L_n = px^2$. Hypothesis and (6) imply n=mq, m odd, $m > 1$. Let $d = (L_m, L_n/L_m)$. (8) implies $d|q$. Lemma 7 implies $d > 1$, so d=q. Therefore $q|L_n$. If (I) holds, then we get a contradiction via Lemma 8, since $pq|L_n$. If (II) holds, then either (i) $L_m = qu^2$, $L_n/L_m = pqv^2$ or (ii) $L_m = pqu^2$, $L_n/L_m = qv^2$ for some u,v. If (i) holds, then (1) and hypothesis imply m=y(q). Now (B) implies there exists a prime, t, such that $t || (L_q/p)$ and $t \nmid y(q)$. If t=p, then $p || (L_q/p)$, so $p^2 | L_q$, contrary to hypothesis. If $t \neq p$, then $t || L_q$, so (14) implies $t || L_{qy(q)}$, that is, $t || px^2$, so $t || x^2$, an impossibility.

If (ii) holds instead, then (6) implies $y(p)|m$ and $y(q)|m$, so $LCM(y(p),y(q))|m$, that is, $LCM(q,y(q))|m$. But (17) implies $LCM(q,y(q))=qy(q)$, so $qy(q)|m$. Since $q^2 \nmid L_{y(q)}$ by hypothesis, we have $q || L_{y(q)}$, so (14) implies $y(q^2)=qy(q)$, hence $y(q^2)|m$. Therefore hypothesis and (6) imply $q^2|L_m$, so that $q|u^2$, which implies $q^2|u^2$, hence $q^3|L_m$. Now (19) and (6) imply $q^2y(q)|m$, so m=qk, $qy(q)|k$. Let $d_1 = (L_k, L_m/L_k)$. Now (8) implies $d_1|q$. Therefore $L_k = ca^2$, where c = 1, p, q, or pq. Since $k < m < n$, (1) implies $c \neq p$, $c \neq pq$. If c=1, then (4) implies k=1 or 3, violating $qy(q)|k$. If c=q, then hypothesis and (1) imply k=y(q), again violating $qy(q)|k$.

THEOREM 19 (*) has no solution if $p \in \{59,359,479,709,719,809,839\}$.

PROOF: In each case, according to [3] and [7], p satisfies the hypothesis of Theorem 18, from which the conclusion follows. Table 2 below gives the details.

Table 2

p	q	y(q)	relevant section of Theorem 18
59	29	7	IIB, t=19489
359	179	89	IIA (see Theorem 10 above)
479	239	119	IIA (see theorem 10 above)
709	59	29	IIA (see first entry in Table 2)
719	359	179	IIA (see second entry in Table 2)
809	101	50	I
839	419	209	IIA (see Theorem 16 above)

We summarize our results in Table 3 below, which contains all solutions of (*) with $2 < p < 1000$.

Table 3

p	n	x^2
3	2	1
7	4	1
11	5	1
19	9	4
29	7	1
47	8	1
199	11	1
521	13	1

Remark: The related results of M. Goldman [8] follow immediately from (1).

ACKNOWLEDGMENT. I wish to thank the referee for his numerous helpful suggestions, as well as for his assistance in obtaining a partial factorization of L_{35312}.

REFERENCES

1. COHN, J.H.E. Square Fibonacci numbers, etc., Fibonacci Quart. v2 n2 91964) 109-113

2. COHN, J.H.E. Squares in some recurrent sequences, Pacific J. Math. v41 n3 (1972) 631-646

3. ALFRED, Brother U. Tables of Fibonacci entry points, Fibonacci Association, 1965

4. LUCAS, E. Theorie des fonctions numeriques simplement periodiques, Amer. J. Math. 1 (1878) 184-240; 289-321

5. ROBBINS, N. Some identities and divisibility properties of linear second order recursion sequences, Fibonacci Quart. 20 (1982) 21-24

6. CARMICHAEL, R.D. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Ann. Math. 15 (1913) 30-70

7. BRILLHART, J. et al Tables of Fibonacci and Lucas factorizations, Math. Comp. 50 (1988) 251-260; S1-S15

8. GOLDMAN, M. On Lucas numbers of the form px^2, where p = 3, 7, 47, or 2207 Math. Reports Canad. Acad. Sci. (June,1988)