A GENERAL CONCLUSION ON LUCAS NUMBERS OF THE FORM px^2 WHERE p IS PRIME

Chizhong Zhou
Yueyang University, Yueyang, Hunan 414000, P. R. China
(Submitted April 1997-Final Revision October 1997)

1. INTRODUCTION

Let L_n be the n^{th} Lucas number, that is, $L_1 = 1$, $L_2 = 3$, $L_{n+1} = L_n + L_{n-1}$ for $n \geq 2$. Let p be prime. Consider the equation

$$L_n = px^2 \quad (n, x > 0). \tag{1.1}$$

In [1], Cohn solved (1.1) for $p = 2$. In [3], Goldman solved (1.1) for $p = 3, 7, 47$, and 2207. In [5], Robbins solved (1.1) for $p < 1000$. He proved that, for $2 < p < 1000$, (1.1) holds iff

$$\begin{aligned}(p, n, x) = {} & (3, 2, 1), (7, 4, 1), (11, 5, 1), (19, 9, 2), \\ & (29, 7, 1), (47, 8, 1)\ (199, 11, 1),\ (521, 13, 1).\end{aligned} \tag{1.2}$$

Besides, he proved that, for $p = 14503$, (1.1) holds iff

$$(n, x) = (28, 7). \tag{1.3}$$

Following Robbins, denote $z(n) = \min\{m : n \mid F_m,\ m > 0\}$, where F_m is the m^{th} Fibonacci number, that is, $F_1 = F_2 = 1$, $F_{m+1} = F_m + F_{m-1}$ for $m \geq 2$. If p is odd and $2 \mid z(p)$, denote $y(p) = \frac{1}{2} z(p)$. Then we observe that every (n, x) in (1.2) and (1.3) satisfies $n = y(p)$. Furthermore, if $2 \mid n$, then either $n = 2^r$ or $n = 2^r q$, where q is an odd prime and $l_{2^r} = q\square$; if $2 \nmid n$, then n is a prime except $n = 9$ for $p = 19$. The question is: Does the above conclusion holds for arbitrary p? Our answer is affirmative. In this paper, we state and prove this general conclusion in Section 3. Some preliminaries are given in Section 2. In Section 4, we give an algorithm which we can use to solve (1.1) for given p. For example, we have given the solutions of (1.1) for $1000 < p < 60000$. A conjecture is also given in Section 4.

2. PRELIMINARIES

Let (n/m) be the Jacobi symbol. (For odd prime m, (n/m) is the Legendre symbol; see [9].) Denote $O_p(n) = k$ if $p^k \| n$.

(1) If $m \geq 2$, then $m \mid F_n$ iff $z(m) \mid n$.

(2) If m is odd and $m \geq 3$, then $m \mid L_n$ iff $n / y(m)$ is an odd integer.

(3) $F_{2n} = L_n F_n$.

(4) $L_{2n} = L_n^2 - 2(-1)^n = 5F_n^2 + 2(-1)^n$.

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

(6) If p is an odd prime, then $z(p) \mid (p - e)$, where $e = (5/p) = 1, -1, 0$ for $p = \pm 1, \pm 2, 0$ (mod 5), respectively.

(7) $L_n \mid L_{kn}$ iff k is odd or $n = 1$.

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

(9) $F_n = (\alpha^n - \beta^n) / (\alpha - \beta)$ and $L_n = \alpha^n + \beta^n$, where $\alpha = (1 + \sqrt{5}) / 2$, $\beta = (1 - \sqrt{5}) / 2$.

(10) If p is an odd prime, $p \mid F_m$ and $p \nmid a$, then $O_p(F_{p^k am} / F_m) = k$.

(11) If p is an odd prime, $p \mid L_m$, a is an odd integer, and $p \nmid a$, then $O_p(L_{p^k am} / L_m) = k$.

(12) $O_2(L_n) = \begin{cases} 1 & \text{if } n = 0 \pmod{6}, \\ 2 & \text{if } n = 3 \pmod{6}, \\ 0 & \text{otherwise.} \end{cases}$

(13) $L_{12m+n} \equiv L_n \pmod{8}$; furthermore, $L_n \equiv 1, -1, 3, -3 \pmod{8}$ for $n = 1, -1$ or $\pm 4, \pm 2$ or $5, -5 \pmod{12}$, respectively.

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

(15) $L_{n+k} + (-1)^k L_{n-k} = L_n L_k$.

(16) If $m > 0$, then $L_{2mk+t} \equiv (-1)^{m(k-1)} L_t \pmod{L_k}$.

Remarks: (1) through (10), (12), (14), and (15) can be found in [4], [8], or [6]; (13) follows from the observation of the sequence $\{L_n \pmod{8}\}$. We give the proofs of (11) and (16) below.

Proof of (11): From (9), it is easy to see that $\sqrt{5}\alpha^m = L_m \alpha + L_{m-1}$. Then

$$(\sqrt{5})^t \alpha^{tm} = \sum_{i=0}^{t} \binom{t}{i} L_{m-1}^{t-i} L_m^i \alpha^i.$$

For the same reason, we have

$$(-\sqrt{5})^t \beta^{tm} = \sum_{i=0}^{t} \binom{t}{i} L_{m-1}^{t-i} L_m^i \beta^i.$$

If $2 \nmid t$, then, by using (9), we get

$$5^{(t-1)/2} L_{tm} / L_m = \sum_{i=1}^{t} \binom{t}{i} L_{m-1}^{t-i} L_m^{i-1} F_i = \sum_{i=1}^{t} h_i. \tag{2.1}$$

Let $t = p^k a$. If $i \ge p^{k+1}$, then $p^{k+1} \mid L_m^{i-1}$ since $p \mid L_m$, whence $p^{k+1} \mid h_i$. If $2 \le i \le p^{k+1}$, let $i = rp^s$ $(p \nmid r,\ s \le k)$, then

$$p^{k-s} \left| \binom{p^k a}{p^s r} = \binom{t}{i} \right. \text{ (see [7], Th. 2.1),}$$

whence $p^{k-s+i-1} \mid h_i$. Since $p \ge 3$, we have $i \ge s+2$, so $k - s + i - 1 \ge k + 1$. Hence, $p^{k+1} \mid h_i$ for $i \ge 2$. Now $h_1 = tL_{m-1}^{t-1}$. Suppose that $p \mid L_{m-1}$, then $p \mid L_m$ and the recurrence $L_{n+1} = L_n + L_{n-1}$ implies $p \mid L_1 = 1$. This is impossible. Hence $p \nmid L_{m-1}$, whence $O_p(h_1) = O_p(t) = k$. Summarizing the above, we have that $p^k \,\|\, \sum_{i=1}^{t} h_i$. From $\{L_n \pmod{5}\}_0^{+\infty} = \{2, 1, 3, 4, 2, 1, \ldots\}$, we observe that $5 \nmid L_m$, thus $p \ne 5$. Then, (11) follows from (2.1). □

Proof of (16): In (15), take $n = k + t$. Then we get $L_{2k+t} \equiv (-1)^{k-1} L_t \pmod{L_k}$. This means that (16) holds for $m = 1$. Assume that (16) holds for m. In (15), taking $n = (2m+1)k + t$, we get $L_{2(m+1)k+t} \equiv (-1)^{k-1} L_{2mk+t} \pmod{L_k}$. By the induction hypothesis, we have

$$L_{(2m+1)k+t} \equiv (-1)^{k-1} (-1)^{m(k-1)} L_t = (-1)^{(m+1)(k-1)} L_t \pmod{L_k},$$

thus (16) is proved. □

Note: (1) through (16) can also be found in [10] which was published in Chinese.

3. THE MAIN RESULT AND ITS PROOF

In the following discussion, we always assume $n, x > 0$.

Theorem: Let p be an odd prime, and $L_n = px^2$, then $n = y(p)$. Furthermore, let $2^r \| y(p)$.

(*a*) If $r = 0$, then $p \equiv \pm 1 \pmod 5$ and $y(p)$ is prime except $y(p) = 9$ for $p = 19$.

(*b*) If $r = 1$, then $(p, n, x) = (3, 2, 1)$.

(*c*) If $r \geq 2$, then $p \equiv 7$ or $23 \pmod{40}$ and either $y(p) = 2^r$ or $y(p) = 2^r q$, where q is an odd prime satisfying $L_2^r = q\square$.

Clearly, the theorem is a considerable improvement of both Theorem 9 and Theorem 11 in [5]. To prove the theorem we need the following lemmas.

Lemma 1: Let p be an odd prime and let $L_n = px^2$. Then $3 \nmid n$ except $n = 9$ for $p = 19$, and so $2 \nmid x$ for $p \neq 19$ (see [5], Th. 3 and Th. 4).

Lemma 2: Let p be prime, $t \equiv \pm 1 \pmod 6$, and $p \equiv \pm L_{5t} \pmod 8$. Then $p \equiv \mp L_t \pmod 4$ and $(2/p)(2/L_t) = -1$.

Proof: If $t \equiv \pm 1 \pmod{12}$, then $5t \equiv \pm 5 \pmod{12}$, whence (13) implies $L_t \equiv \pm 1 \pmod 8$ and $L_{5t} \equiv \pm 3 \pmod 8$. Hence, the lemma holds. If $t \equiv \pm 5 \pmod{12}$, the lemma is proved in the same way. $\square$

Lemma 3: Let p be prime, $n = (12s \pm 1)t$, $s > 0$, $t \equiv \pm 1 \pmod 6$, and $p \mid L_t$. Then $L_n \neq px^2$.

Proof: Suppose $L_n = px^2$. Then, from (13) and (5), we have $L_n \equiv L_{\pm t} \equiv \pm L_t \pmod 8$. (12) implies $2 \nmid L_n$, $2 \nmid L_t$, so $2 \nmid x$. Thus,

$$p \equiv L_n \equiv \pm L_t \pmod 8. \tag{3.1}$$

Rewrite $n = 2 \cdot 3^a \cdot k \pm t$, where $k \equiv \pm 2 \pmod 6$. From (16), it follows that

$$px^2 = L_{2 \cdot 3^a \cdot k \pm t} \equiv -L_{\pm t} = \mp L_t \pmod{L_k} \tag{3.2}$$

It is easy to see that $k = 2ht$. (16) implies $L_k = L_{2ht+0} \equiv L_0 = 2 \pmod{L_t}$. This and $2 \nmid L_t$ imply $(L_k, L_t) = 1$. Since $p \mid L_t$, we have $L_k \equiv 2 \pmod p$ and $(L_k, p) = 1$. (13) implies $L_k \equiv -1 \pmod 4$. From (3.1), we have

$$\begin{aligned} (p(\mp L_t)/L_k) &= \mp(p/L_k)(L_t/L_k) = (\mp)(\pm)(L_k/p)(L_k/L_t) \\ &= -(L_k/p)(L_k/L_t) = -(2/p)(2/L_t) = -1. \end{aligned}$$

This contradicts (3.2). Hence, $L_n \neq px^2$. $\square$

Lemma 4: Let p be prime, $n = (12s \pm 5)t$, $t \equiv \pm 1 \pmod 6$, and $p \mid L_t$. Then $L_n \neq px^2$.

Proof: Suppose $L_n = px^2$. For the same reason as in the proof of Lemma 3, we have

$$p \equiv L_n \equiv \pm L_{5t} \pmod 8. \tag{3.3}$$

Rewrite $n = 2(6s \pm 2)t \pm t = 2k \pm t$. Then (16) implies

$$px^2 = L_{2k \pm t} \equiv -L_{\pm t} = \mp L_t \pmod{L_k}. \tag{3.4}$$

For the same reason as above, $L_k \equiv 2 \pmod{L_t}$ and $L_k \equiv 2 \pmod{p}$, $(L_k, L_t) = (L_k, p) = 1$, and $L_k \equiv -1 \pmod 4$. Thus, from Lemma 2, we have

$$(p(\mp L_t)/L_k) = \mp(p/L_k)(L_t/L_k) = (\mp)(\mp)(L_k/p)(L_k/L_t) = (2/p)(2/L_t) = -1.$$

This contradicts (3.4). Hence, $L_n \neq px^2$. □

Lemma 5: Let p be prime, $n = (12s \pm 5)t$, $t = 2^r d$, $r \geq 2$, $d \equiv \pm 1 \pmod 6$, and $p \mid L_t$. Then $L_n \neq px^2$.

Proof: Suppose $L_n = px^2$. Since $2^r = 4 \cdot 2^{r-2} \equiv 4(-1)^{r-2} = \pm 4 \pmod{12}$ for $r \geq 2$, we have $n \equiv \pm 5t \equiv \mp t \equiv \pm 4$ or $\mp 4 \pmod{12}$. (13) implies $L_n \equiv L_t \equiv -1 \pmod 8$, and so $L_n = px^2$ implies $p \equiv -1 \pmod 8$. Let $3s \pm 1 = 2^a m$, $2 \nmid m$. Then $n = 2m \cdot 2^{a+1} t \pm t = 2mk \pm t$. (16) implies

$$px^2 = L_n \equiv -L_{\pm t} = -L_t \pmod{L_k}. \tag{3.5}$$

Again, (16) implies $L_k = L_{2 \cdot 2^a t + 0} \equiv (-1)^{2^a(t-1)} L_0 = \pm 2 \pmod{L_t}$, and so $L_k \equiv \pm 2 \pmod{p}$. For the same reason as given above, $L_k \equiv -1 \pmod 8$ and $(L_k, L_t) = (L_k, p) = 1$. Thus,

$$(p(-L_t)/L_k) = -(p/L_k)(L_t/L_k) = -(-1)(L_k/p)(-1)(L_k/L_t) = -(\pm 2/p)(\pm 2/L_t) = -1$$

This contradicts (3.5). Hence, $L_n \neq px^2$. □

Lemma 6: Let p be prime, $n = (12s \pm 1)t$, $t = 2^r d$, $s > 0$, $r \geq 2$, $d \equiv \pm 1 \pmod 6$, and $p \mid L_t$. Then $L_n \neq px^2$.

Proof: Suppose $L_n = px^2$. Let $3s = 2^a m$, $2 \nmid m$. Then $n = 2 \cdot m \cdot 2^{a+1} t \pm t = 2mk \pm t$. The proof is completed in the same way as the proof of Lemma 5. □

Lemma 7: Let p be an odd prime, and $L_n = px^2$. Then $n = y(p)$.

Proof: From (1.2), we know that the lemma holds for $p = 19$. Now we assume that $p \neq 19$. Then Lemma 1 implies $3 \nmid n$ and (2) implies $n = mt$, where $t = y(p)$ and $2 \nmid m$. Therefore, $m \equiv \pm 1 \pmod 6$. If $m > 1$, then $m = 12s \pm 1$ or $m = 12s \pm 5$. Let $t = 2^r d$, $r \geq 0$, $d \equiv \pm 1 \pmod 6$. When $r = 0$, the conditions of Lemma 3 and Lemma 4 are fulfilled. When $r \geq 2$, the conditions of Lemma 5 and Lemma 6 are fulfilled. These all lead to $L_n \neq px^2$. Hence, $m = 1$, and so $n = y(p)$. When $r = 1$, (12) implies $3 \,\|\, L_n$, whence $L_n = px^2$ iff $(p, n, x) = (3, 2, 1)$. Obviously, $2 = y(3)$, and we are done. □

Lemma 8: Let p be prime, $p > 3$, and $t = y(p) \equiv \pm 1 \pmod 6$. If $L_t = px^2$, then $p \equiv \pm 1 \pmod 5$ and t is prime.

Proof: $L_t = px^2$, $2 \nmid t$, and (4) imply $5F_t^2 \equiv 4 \pmod p$. This implies $(5/p) = 1$, and so $p \equiv \pm 1 \pmod 5$. Suppose that t is a composite. Then $t = kq$, where q is a prime greater than 3, and $k > 1$. (14) implies $L_q \neq \square$. Since $2 \nmid L_q$, there exists an odd prime r such that $r \mid L_q$ and $2 \nmid O_r(L_q)$. From (2), it is clear that

$$y(r) = q. \tag{3.6}$$

If $r = q$, then $z(q) = 2 \cdot y(q) = 2 \cdot y(r) = 2q$. (6) implies $2q \mid (q - (5/q))$. This is impossible. Hence, $r \neq q$. If $r \nmid k$, then (11) implies $O_r(L_{kq}) = O_r(L_q)$. Therefore, $2 \nmid O_r(L_t)$. This means that

$L_t = px^2$ implies $r = p$. Thus, from (3.6), we get $y(p) = q < kq = y(p)$. This is a contradiction! Hence, $r \mid k$. Let $k = rh$, then $L_{qh} \cdot L_{qrh} / L_{qh} = px^2$. Let $(L_{qh}, L_{qrh} / L_{qh}) = d$. (8) implies $d \mid r$, (2) implies $r \mid L_{qh}$, and so (11) implies $O_r(L_{qrh} / L_{qh}) = 1$. Thus, $r \mid d$; hence, $d = r$. Then we have either (i) $L_{qh} = ru^2$ or (ii) $L_{qh} = rpu^2$. (ii) contradicts the fact that $y(p) = qrh$, since $qh < y(p)$. If (i) holds, then, from Lemma 7, we have $y(r) = qh$. Comparing it with (3.6), we get $h = 1$ and $t = qr$.

For the same reason, there exists an odd prime s such that $s \mid L_r$ and $2 \nmid O_s(L_r)$. And we also have

$$y(s) = r \tag{3.7}$$

and $s \neq r$. Again, for the same reason as $r \mid k$, we have $s \mid q$, whence $s = q$. Thus, (3.7) becomes

$$y(q) = r. \tag{3.8}$$

Equations (3.6) and (3.8) imply that $z(r) = 2q$ and $z(q) = 2r$. Thus, (6) implies $2q \mid (r - (5/r))$ and $2r \mid (q - (5/q))$. Clearly, this is impossible. Hence, t is prime. □

Lemma 9: Let p be prime, $p > 3$, $2^r \| t = y(p)$, and $r \geq 2$. If $L_t = px^2$, then $p \equiv 7$ or 23 (mod 40) and either $t = 2^r$ or $t = 2^r q$, where q is a prime satisfying $l_{2^r} = q\square$.

Proof: From the proof of Lemma 7, we know that $t = 2^r d$, $d \equiv \pm 1$ (mod 6). From the proof of Lemma 5, we know that $p \equiv -1$ (mod 8). $L_t = px^2$, $2 \mid t$, and (4) imply $5F_t^2 \equiv -4$ (mod p), and so $(-5/p) = -(5/p) = 1$. This leads us to $p \equiv \pm 2$ (mod 5). Summarizing the above, we obtain $p = 7$ or 23 (mod 40).

From the proof of Lemma 8, we know that there exists an odd prime q such that $q \mid l_{2^r}$ and $2 \nmid O_q(l_{2^r})$. From (2), it is clear that $y(q) = 2^r$. If $d \neq 1$, then, for the same reason as in the proof of Lemma 8, we have $q \mid d$. Let $d = qh$, then $l_{2^r h} \cdot l_{2^r qh} / l_{2^r h} = px^2$. Now (8), (2), and (11) imply $(l_{2^r h}, l_{2^r qh} / l_{2^r h}) = q$, so we get either (i) $l_{2^r h} = qu^2$ or (ii) $l_{2^r h} = qpu^2$. (ii) contradicts the fact that $y(p) = 2^r qh$. If (i) holds, then Lemma 7 implies $y(q) = 2^r h$. Comparing this with $y(q) = 2^r$, we get $h = 1$ and $l_{2^r} = qu^2$. Thus, the lemma is proved. □

Proof of the Theorem: The Theorem follows from Lemmas 7 through 9. □

4. AN ALGORITHM AND EXAMPLES

From the Theorem in Section 3 and using (1) and (6), we can give the following algorithm.

Algorithm: Let p be a given odd prime, $p \neq 3$, 19.

I. If $p \not\equiv \pm 1$ (mod 5) and $p \not\equiv 7, 23$ (mod 40), then (1.1) has no solution.

II. For $p \equiv \pm 1$ (mod 5), let $A = \{q_1, \ldots, q_k\}$ be the set of distinct prime factors greater than 3 of $p - 1$.

- *(a)* If A is empty, then (1.1) has no solution.
- *(b)* For $i = 1, \ldots, k$, calculate L_{q_i} (mod p).
- *(c)* If there exists an $i = j$ such that $L_{q_j} \equiv 0$ (mod p), then calculate L_{q_j}. If $L_{q_j} = pu^2$ $(u > 0)$, then $(n, x) = (q_j, u)$ is the solution of (1.1), otherwise (1.1) has no solution.
- *(d)* If, for all $i = 1, \ldots, k$, $L_{q_i} \not\equiv 0$ (mod p), then (1.1) has no solution.

III. For $p \equiv 7$ or 23 (mod 40), let $2^a \| (p+1)$ and $A = \{q_1, \ldots, q_k\}$ be the set of distinct prime factors greater than 3 of $p+1$.

- ***(a)*** For $s = 2, 3, \ldots, a-1$, calculate l_{2^s} (mod p).
- ***(b)*** If there exists an $s = r$ such that $l_{2^r} \equiv 0$ (mod p), then calculate l_{2^r}. If $l_{2^r} = pu^2$ $(u > 0)$, then $(n, x) = (2^r, u)$ is the solution of (1.1), otherwise (1.1) has no solution.
- ***(c)*** If, for all $s = 2, 3, \ldots, a-1$, $l_{2^r} \not\equiv 0$ (mod p), then $s = 2, 3, \ldots, a-1$ and, for every q_i in A such that $q_i \equiv 7$ or 23 (mod 40), calculate l_{2^s} (mod q_i). Let B be the set of such (s, i)'s that $l_{2^s} = q_i\square$.
- ***(d)*** If B is empty, then (1.1) has no solution.
- ***(e)*** For each (s, i) in B, calculate $L_{2^s q_i}$ (mod p).
- ***(f)*** If there exists an $(s, i) = (r, j)$ in B such that $L_{2^r q_j} \equiv 0$ (mod p), then calculate $L_{2^r q_j}$. If $L_{2^r q_j} \equiv pu^2$ $(u > 0)$, then $(n, x) = (2^r q_j, u)$ is a solution of (1.1), otherwise (1.1) has no solution.
- ***(g)*** If, for all (s, i) in B, $L_{2^s q_i} \not\equiv 0$ (mod p), then (1.1) has no solution.

Remark: For calculating L_m (mod p) and L_m, there is an algorithm that determines the result after $[\log_2 m]$ recursive calculations (see [2]).

Example 1: $p = 63443 \not\equiv \pm 1$ (mod 5) and $p \not\equiv 7, 23$ (mod 40). Hence, (1.1) has no solution.

Example 2: $p = 19489 \equiv -1$ (mod 5), $p - 1 = 2^5 \times 3 \times 7 \times 29$, $A = \{7, 29\}$. By calculating, we get $L_{29} \equiv 0$ (mod p). But $L_{29} = 59p \neq px^2$, so (1.1) has no solution.

Example 3: $p = 4481 \equiv 1$ (mod 5), $p - 1 = 2^9 \times 5 \times 7$, $A = \{5, 7\}$. Since $L_5, L_7 \not\equiv 0$ (mod p), (1.1) has no solution.

Example 4: $p = 9349 \equiv -1$ (mod 5), $p - 1 = 2^2 \times 3 \times 19 \times 41$, $A = \{19, 41\}$. By calculating, we get $L_{19} \equiv 0$ (mod p) and $L_{19} = p$. Hence, $(n, x) = (19, 1)$ is the solution of (1.1).

Example 5: $p = 1103 \equiv 23$ (mod 40), $p + 1 = 2^4 \times 3 \times 23$, $A = \{23\}$. Since $l_{2^2}, l_{2^3} \not\equiv 0$ (mod p) and $l_{2^2}, l_{2^3} \not\equiv 0$ (mod 23), (1.1) has no solution.

Example 6: $p = 1097 \equiv 7$ (mod 40), $p + 1 = 2^6 \times 17$, $A = \{17\}$. Since $l_{2^5} \equiv 0$ (mod p) but $l_{2^5} = 1087 \times 4481 \neq px^2$, (1.1) has no solution.

Example 7: $p = 3607 \equiv 7$ (mod 40), $p + 1 = 2^3 \times 11 \times 41$, $A = \{11, 41\}$. Since $l_{2^2}, l_{2^3} \not\equiv 0$ (mod p) and 11 and $41 \not\equiv 7, 23$ (mod 40), (1.1) has no solution.

Example 8: $p = 14503 \equiv 23$ (mod 40), $p + 1 = 2^3 \times 7^2 \times 37$, $A = 7, 37\}$. By the Algorithm, we get $l_{2^2} = 7$ and $l_{2^2 \cdot 7} = p \cdot 7^2$. Hence, $(n, x) = (28, 7)$ is a solution of (1.1).

Remark: In II(c), III(b), and III(d) of the Algorithm, it is unnecessary to calculate L_t, where $t = q_j$, 2^r, or $2^r q_j$ for most of the t's. The reason is that, if pL_t is a quadratic nonresidue (mod *m*), where *m* is some prime, then $L_t \neq px^2$. For example, by using the Algorithm and making *m* run through the first 20 odd primes, and by means of a computer, we have verified the following proposition.

Proposition: Let p be prime, $10^3 < p < 6 \times 10^4$. Then (1.1) holds iff

$$(p, n, x) = (2207, 16, 1),\ (3571, 17, 1),\ (9349, 19, 1),\ (14503, 28, 7). \tag{4.1}$$

Extensive numeric results inspire the following conjecture.

Conjecture: Let p be an odd prime and $p \neq 3$, 19. Then $L_n = px^2$ iff one of the following conditions holds:

(a) $p \equiv \pm 1 \pmod 5$, $y(p)$ is prime, and $L_{y(p)} = p$, so $(n, x) = (y(p), 1)$;

(b) $p \equiv 7$ or 23 (mod 40), $y(p) = 2^r$, and $L_{y(p)} = p$, so $(n, x) = (y(p), 1)$;

(c) $p \equiv 7$ or 23 (mod 40), $y(p) = 2^r q$, where q is a prime greater than 3 satisfying $l_{2^r} = q$ and $L_{y(p)} = pq^2$, so $(n, x) = (y(p), q)$.

We point out that the conjecture would hold if we could show $p^2 \nmid L_{y(p)}$ for all odd prime p. At this time, it remains unknown whether there exists an odd prime p such that $p^2 \mid L_{y(p)}$.

REFERENCES

1. J. H. E. Cohn. "Square Fibonacci Numbers, etc." *The Fibonacci Quarterly* **2.2** (1964):109-13.
2. A. Di Porto & P. Filipponi. "More on the Fibonacci Pseudoprimes." *The Fibonacci Quarterly* **27.2** (1989):232-42.
3. M. Goldman. "On Lucas Numbers of the Form px^2, Where $p = 3, 7, 47$, or 2207." *Math. Reports Canada Acad. Sci.* (June 1988).
4. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969.
5. N. Robbins. "Lucas Numbers of the Form px^2, Where p Is Prime." *Internatl. J. Math. & Math. Sci.* **14.4** (1991):697-704.
6. N. Robbins. "Fibonacci Numbers of the Form cx^2, Where $1 \leq p \leq 1000$." *The Fibonacci Quarterly* **28.4** (1990):306-15.
7. N. Robbins. "Some Congruence Properties of Binomial Coefficients and Linear Second Order Recurrence." *Internatl. J. Math. & Math. Sci.* **11.4** (1988):743-50.
8. S. Vajda. *Fibonacci and Lucas Numbers, and the Golden Section*. Chichester: Ellis Horwood Ltd., 1989.
9. I. M. Vinogradov. *Elements of Number Theory*. New York: Dover, 1954.
10. Chizhong Zhou. *Fibonacci-Lucas Sequences and Their Application* (in Chinese). China: Hunan Science and Technology Publishing House, 1993. (MR. 95m: 11027)

AMS Classification Number: 11B39