COLLOQUIUM MATHEMATICUM

VOL. 78 1998 NO. 1

SQUARES IN LUCAS SEQUENCES HAVING AN EVEN FIRST PARAMETER

BY

PAULO RIBENBOIM (KINGSTON, ONTARIO) AND
WAYNE L. McDANIEL (ST. LOUIS, MISSOURI)

1. Introduction. Let P and Q be non-zero relatively prime integers, α and β ($\alpha > \beta$) be the zeros of $x^2 - Px + Q$, and, for $n \ge 0$, let

$$(0)\qquad U_n = U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta},\qquad V_n = V_n(P,Q) = \alpha^n + \beta^n.$$

It is known that there exist only a finite number of integers n such that $U_n(P,Q)$ is a square ($=\square$); however, the bound on n, although effectively computable, is, in general, extremely large [6]. If P and Q are *odd* integers, the square terms of the sequence $\{U_n(P,Q)\}$ are known [8]. Much less is known when P is even: for an arbitrary even P, the square terms are only known when $Q = 1$ or $Q = P - 1$, and when $Q = -1$ it is known that $\{U_n(P,Q)\}$ has at most two square terms. These results are derived from W. Ljunggren's work concerning certain Diophantine equations (see [2], [3], [4], and, also, [5]).

If $Q \ne \pm 1$ or $P - 1$, and P is even, the best result in the effort to solve $U_n(P,Q) = \square$ was obtained in 1983 when Rotkiewicz [10] showed that if P is even and $Q \equiv 1 \pmod 4$, then $U_n(P,Q) = \square$ only if n is an odd square or an even integer $\ne 2^{k+1}$ whose largest prime factor divides the discriminant D ($= P^2 - 4Q$).

In this paper, we improve upon Rotkiewicz's results by showing that if P is even and $Q \equiv 1 \pmod 4$, then, for $n > 0$, $U_n(P,Q) = \square$ only if all the prime factors of n belong to a small known finite set: each is a prime factor of D. We show, further, that if p is a prime and $p^{2t} \mid n$, then $U_{p^{2u}}$ is a square for $u = 1, \ldots, t$. In addition, for even values of n, we show that $U_n = \square$ only if $P = \square$ or $2\square$. Finally, we obtain corresponding results for $U_n = 2\square$. At the end of the paper, we give several infinite sets of pairs (P,Q) for which $U_n(P,Q) \ne \square$ for $n > 2$.

1991 *Mathematics Subject Classification*: Primary 11B39.

MAIN THEOREM. *Let $n > 0$. If P is even, $Q \equiv 1 \pmod 4$, and $U_n = \Box$, then n is a square, or twice an odd square, and all prime factors of n divide D; if $p^t > 2$ is a prime divisor of n and $1 \le u \le t$, then $U_{p^u} = \Box$ if u is even and $U_{p^u} = p\Box$ if u is odd. If n is even, then $U_n = \Box$ only if, in addition, $P = \Box$ or $2\Box$.*

2. Restrictions, notation and preliminary results. We shall assume throughout this paper that P is even, $Q \equiv 1 \pmod 4$, $\gcd(P,Q) = 1$ and $D = P^2 - 4Q > 0$.

We use the recursive relations $U_n = PU_{n-1} - QU_{n-2}$ and $V_n = PV_{n-1} - QV_{n-2}$ and the following properties. Let n and m be positive integers, q be an odd prime, and $\varrho(q)$ be the entry point of q (i.e., $q \mid U_{\varrho(q)}$ and $q \nmid U_n$ if $n < \varrho(q)$).

(1) U_n is even iff n is even; V_n is even.
(2) If $q \mid U_n$, then $\varrho(q) \mid n$.
(3) $q \mid U_q$ iff $q \mid D$.
(4) If $q \mid U_k$, for some $k > 0$, and $q \nmid D$, then $q \mid U_{q-1}$ or $q \mid U_{q+1}$.
(5) $\gcd(U_n, U_m) = U_{\gcd(n,m)}$, and $U_n \mid U_m$ iff $n \mid m$.
(6) If $q^e \parallel U_n$, then $q^{e+1} \parallel U_{nq}$.
(7) $\gcd(U_n, Q) = \gcd(V_n, Q) = 1$.
(8) If n is odd, then $\gcd(U_n, P) = 1$.
(9) If $d = \gcd(m,n)$, then $\gcd(V_m, V_n) = V_d$ if m/d and n/d are odd, and 2 otherwise.
(10) If $d = \gcd(m,n)$, then $\gcd(U_m, V_n) = V_d$ if m/d is even, and 1 or 2 otherwise.
(11) $U_{2m} = U_m V_m$.
(12) If n is odd, then $U_n = \Box$ only if $n = \Box$.

Property (12) was proven by Rotkiewicz [10] and the other properties are well known (see e.g. [7], p. 44).

LEMMA 1. *If q is an odd prime and each prime factor of the odd integer m is greater than q, then $q \nmid U_m$.*

P r o o f. Assume each prime factor of m is greater than the odd prime q. By (3) and (4), if $q \mid U_m$, then q divides U_q, U_{q-1}, or U_{q+1}; but then, by (2), $\varrho(q)$ divides q, $q-1$ or $q+1$, implying that each prime factor of $\varrho(q)$ is $\le q < m$. However, this is impossible, since, by (2), $q \mid U_m$ implies that $\varrho(q) \mid m$.

Robbins [9] has shown that for all positive integers m and n, there exists an integer R such that $U_{mn}/U_m = [n(QU_{m-1})^{n-1} + U_m R]$. Since $\gcd(U_m, QU_{m-1}) = 1$, we immediately have:

LEMMA 2. *For all positive integers m and n,* $\gcd(U_m, U_{mn}/U_m) = \gcd(U_m, n)$.

LEMMA 3. *If* $2 \parallel P$, *then*

$$V_n \equiv \begin{cases} P \pmod 8 & \text{if } n \text{ is odd}, \\ 2 \pmod 8 & \text{if } n \text{ is even.} \end{cases}$$

If $4 \mid P$, *then*

$$V_n \equiv \begin{cases} P \pmod 8 & \text{if } n \text{ is odd}, \\ 2 \pmod 8 & \text{if } n \equiv 0, 4 \pmod 8, \\ -2 \pmod 8 & \text{if } n \equiv 2, 6 \pmod 8. \end{cases}$$

Proof. By (0), $V_0 = 2$, $V_1 = P$ and $V_2 = P \cdot P - Q \cdot 2 \equiv P^2 - 2 \pmod 8$. Assume that $2 \parallel P$, and that the lemma holds for all integers $< n$. If $n \geq 2$ is odd, then

$$V_n = PV_{n-1} - QV_{n-2} \equiv \begin{Bmatrix} 2P - QP \text{ or} \\ 2P - 5QP \end{Bmatrix} \equiv P \text{ or } 5P \pmod 8,$$

and for $P \equiv \pm 2 \pmod 8$ we have $5P \equiv P \pmod 8$. If $n \geq 2$ is even, then

$$V_n = PV_{n-1} - QV_{n-2} \equiv 4 - Q \cdot 2 \equiv 2 \pmod 8.$$

The proof for $4 \mid P$ is similar.

3. Proofs of the theorems

THEOREM 1. *Let* $n = 2^k m$, $k \geq 1$ *and* m *odd.*

(a) *If* $2 \parallel P$, *then* $U_n = \square$ *only if* k *is even and* $U_m = \square$.
(b) *If* $4 \mid P$, *then* $U_n = \square$ *only if* $k = 1$ *and* $U_m = \square$.

Proof. Assume that $U_n = U_{2^k m} = \square$. By (11),

$$U_n = U_m V_m V_{2m} V_{4m} \ldots V_{2^{k-1}m},$$

and since, by (9) and (10), $\gcd(U_m, V_{2^j m}) = 1$, and $\gcd(V_{2^i m}, V_{2^j m}) = 2$ for $0 \leq i < j \leq k-1$, each factor is $\square$ or $2\square$; in particular, since U_m is odd, $U_m = \square$. Now, if $2 \parallel P$, then, since, by Lemma 3, $V_{2^i m} \equiv 2 \pmod 4$ for $0 \leq i \leq k-1$, it follows that $V_{2^i m} = 2\square$ and k is even. If, on the other hand, $4 \mid P$, then, by Lemma 3, $V_{2m} \equiv -2 \pmod 8$, so $V_{2m} \neq \square$ or $2\square$, and it follows that $k = 1$.

LEMMA 4. *Assume p is a prime, t is a positive integer,* $p^t > 2$, *and* $U_{p^t} = \square$. *Then* $p \mid D$, *and if* $1 \leq u \leq t$, *then* $U_{p^u} = \square$ *if u is even and* $U_{p^u} = p\square$ *if u is odd.*

Proof. By Lemma 2,

$$d = \gcd(U_{p^u}, U_{p^t}/U_{p^u}) = \gcd(U_p, p^{t-u}),$$

so, for some s $(0 \le s \le t-1)$, $d = p^s$; hence, $\square = U_{p^t} = U_{p^u} \cdot (U_{p^t}/U_{p^u})$ implies that $U_{p^u} = p^s\square = \square$ or $p\square$. Since, by (12) if p is odd and by Theorem 1(a) if $p = 2$ (note that $p^t > 2$), U_{p^u} is a square only if u is even, we have $U_{p^u} = p\square$ if u is odd, and in view of (6), $U_{p^u} = \square$, if u is even. Since $U_p = p\square$, it follows from (3) that $p \mid D$ if p is odd, and $p \mid D$ trivially if $p = 2$ since D is even.

THEOREM 2. *Let $n > 1$ and assume that $U_n = \square$. If p is a prime factor of n, then $p \mid D$. Further, if $p^t \parallel n$ and $p^t > 2$, then, for $1 \le u \le t$, $U_{p^u} = \square$ if u is even, and $U_{p^u} = p\square$ if u is odd.*

Proof. Let $n = m_0 m$, where m_0 is such that each prime divisor of m_0 is less than the least prime divisor of m. Let

$$d = \gcd(U_m, U_{mm_0}/U_m) = \gcd(U_m, m_0).$$

Clearly, if $m_0 = 1$ then $d = 1$. If $m_0 > 1$ then m is odd (and U_m is odd) and either $d = 1$ or some odd prime factor p of m_0 divides U_m; however, since each prime factor of m is $> p$, the latter is impossible by Lemma 1. So $d = 1$, and $\square = U_n = U_m(U_{mm_0}/U_m)$ implies $U_m = \square$.

Now, let $n = p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}$, $p_i < p_j$ for $i < j$. We have just shown, in particular, that $U_{p_r^{t_r}} = \square$, and therefore $p_r \mid D$, by Lemma 4. If $r > 1$, let $a < r$ be such that $p_{a+1}, p_{a+2}, \ldots, p_r$ divide D. Let $m = \prod_{i=a}^{r} p_i^{t_i}$, and set

$$d' = \gcd(U_{p_a^{t_a}}, U_m/U_{p_a^{t_a}}) = \gcd(U_{p_a^{t_a}}, m/p_a^{t_a}).$$

Now, if $a < k \le r$, then $p_k \nmid U_{p_a^{t_a}}$, since, by (2) and (3), $\varrho(p_k) = p_k$. Hence, $d' = 1$ and $U_{p_a^{t_a}} = \square$. By induction, we have $U_{p_i^{t_i}} = \square$ for $i = 1, \ldots, r$. The theorem then follows from Lemma 4.

We now show that unless P or $2P$ is restricted to the set of perfect squares, $U_n \ne \square$ for n an even positive integer.

LEMMA 5. *For any fixed integer Q and every positive integer n, $V_n = f_n(P)$, where $f_n(P)$ is a polynomial in P; for each $k \ge 1$, the term of lowest degree of $f_{2k}(P)$ is $(-1)^k Q^k$, and of $f_{2k+1}(P)$ is $(-1)^k(2k+1)Q^k P$.*

The proof is by induction on k.

By this lemma, if m is odd, $V_m/P = AP \pm mQ^{(m-1)/2}$, for some integer A. If, now, $U_m = \square$, then, since each prime factor of m divides D $(= P^2 - 4Q)$ by Theorem 2, we have $\gcd(P, m) = \gcd(D, m) = 1$, and it follows that $\gcd(P, V_m/P) = 1$. Hence, if $P \cdot V_m/P = V_m = \square$, then $P = \square$, and if $V_m = 2\square$, then $P = 2\square$.

THEOREM 3. *Assume $n > 0$ is an even integer and $U_n = \square$. If $2 \parallel P$, then $P = 2\square$, and if $4 \mid P$, then $P = \square$.*

Proof. Let $n = 2^k m$, m odd. If $2 \parallel P$, then, as seen in the proof of Theorem 1, $V_m = 2\square$, so, by the remarks preceding the theorem, $P = 2\square$. If

$4 \mid P$, then $k=1$ by Theorem 1, so $U_n = U_{2m} = U_m V_m$, and since $U_m = \square$, we have $V_m = \square$, and $P = \square$.

The Main Theorem incorporates the results of Theorems 1, 2 and 3. Similar results can be obtained for the sequence $\{2U_n(P,Q)\}$:

THEOREM 4. *Let* $n = 2^k m$, $k \geq 0$ *and* m *odd.*

(a) *If* $k = 0$ (*i.e.*, n *is odd*), *then* $U_n \neq 2\square$.
(b) *If* $2 \parallel P$, *then* $U_n = 2\square$ *only if* k *is odd*, $U_m = \square$ *and* $P = 2\square$.
(c) *If* $4 \mid P$, *then* $U_n = 2\square$ *only if* $k = 1$, $U_m = \square$ *and* $P = 2\square$.

Proof. Assume that $U_n = U_{2^k m} = 2\square$. Trivially, if $k = 0$, then $U_n \neq 2\square$ since U_n is odd. Thus $k \geq 1$. Then $U_n = U_m V_m V_{2m} \dots V_{2^{k-1}m}$ implying that $U_m = \square$. The remainder of the proof parallels that of Theorems 1 and 3.

EXAMPLE 1. Let r be a positive odd integer, $P = 2r$, and $Q = r^2 - 4$. Then $\gcd(P,Q) = 1$ and $Q \equiv 1 \pmod 4$. Since $D = P^2 - 4Q = 4r^2 - 4(r^2-4) = 16$, the only prime factor of $2D$ is $p = 2$. Now, $U_4 = P(P^2 - 2Q) = \square$ only if $P^2 - 2Q = 2\square$. But

$$P^2 - 2Q = 4r^2 - 2(r^2 - 4) = 2(r^2 + 4) \neq 2\square.$$

By Theorems 1 and 2, then, the only squares in $\{U_n(2r, r^2 - 4)\}$ are U_0 and U_1.

EXAMPLE 2. Let r be a positive integer, $3 \nmid r$, $P = 4r$, and $Q = 4r^2 - 3$. Then $\gcd(P,Q) = 1$, $Q \equiv 1 \pmod 4$ and $D = 16r^2 - 4(4r^2 - 3) = 12$. Now

$$U_3 = P^2 - Q = 16r^2 - (4r^2 - 3) = 3(4r^2 + 1) \neq 3\square,$$

so $U_n = \square \;\Rightarrow\; 3 \nmid n$. By Theorems 1, 2 and 3, $U_n = \square$ iff $n = 0$, 1, or 2, with $U_2 = \square$ iff $r = \square$.

No example is known of a pair P, Q and an odd prime p such that $U_{p^2} = \square$ (and none exists if P and Q are odd). It is our conjecture that none exists if P is even and $Q \equiv 1 \pmod 4$; that is, that the only odd value of n such that $U_n = \square$ is $n = 1$. It appears highly probable that, in practice, one can easily determine all n such that $U_n(P,Q) = \square$ for any given P and Q such that U_{p^2} is computable for the largest prime factor p of $P^2 - 4Q$—and know that all have been found.

REFERENCES

[1] J. H. E. Cohn, *Squares in some recurrent sequences*, Pacific J. Math. 41 (1972), 631–646.

[2] W. Ljunggren, *Über die unbestimmte Gleichung* $Ax^2 - By^4 = C$, Arch. Math. Naturvid. 41 (1938), 3–18.

[3] W. Ljunggren, *Zur Theorie der Gleichung* $x^2+1=Dy^4$, Avh. Norske Vid. Akad. Oslo. I, No. 5 (1942), 1–26.

[4] —, *New propositions about the indeterminate equation* $\frac{x^n-1}{x-1}=y^q$, Norske Mat. Tidskr. 25 (1943), 17–20.

[5] L. J. Mordell, *Diophantine Equations*, Pure Appl. Math. 30, Academic Press, London, 1969.

[6] A. Pethő, *Perfect powers in second order linear recurrences*, J. Number Theory 15 (1982), 5–13.

[7] P. Ribenboim, *The Book of Prime Number Records*, Springer, New York, 1989.

[8] P. Ribenboim and W. L. McDaniel, *The square terms in Lucas sequences*, J. Number Theory 58 (1996), 104–123.

[9] N. Robbins, *Some identities and divisibility properties of linear second-order recursion sequences*, Fibonacci Quart. 20 (1982), 21–24.

[10] A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, Acta Arith. 42 (1983), 163–187.

Department of Mathematics
Queen's University
Kingston, Ontario
Canada K7L 3N6

Department of Mathematics and Computer Science
University of Missouri-St. Louis
St. Louis, Missouri 63121
U.S.A.
E-mail: mcdaniel@arch.umsl.edu

Received 30 December 1997