ACTA ARITHMETICA
C.1 (2001)

Squares in Lehmer sequences and some Diophantine applications

by

Florian Luca (Morelia) and P. G. Walsh (Ottawa)

I. Introduction. In his seminal paper [6], extending the theory of Lucas functions, D. H. Lehmer studied a wide class of sequences, which are commonly referred to as *Lehmer sequences*. Let $L > 0$ and M be rational integers such that $L - 4M > 0$ and $(L, M) = 1$. Let α and β be the two roots of the trinomial $x^2 - \sqrt{L}\,x + M$. For a non-negative integer n, the nth term in the Lehmer sequence $\{P_n\}$ (see [6]) is given by

$$P_n := P_n(\alpha,\beta) = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{for } n \text{ odd,} \\[2ex] \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{for } n \text{ even.} \end{cases} \tag{1.1}$$

Lehmer sequences have many interesting properties and often arise in the study of exponential Diophantine equations. A thorough analysis of the arithmetic properties of the numbers P_n was initiated by Lehmer. It is not difficult to see that P_n is a positive integer for all positive integers n, and moreover that P_m divides P_n whenever m divides n.

In this paper, we investigate the occurrence of squares and certain square-classes in Lehmer sequences. This type of problem has received considerable interest, most notably in the work of Cohn [2], [3], and Ribenboim and McDaniel [10], [11]. Some of the more general results, whose consequences have been rediscovered in many papers, are those of Rotkiewicz [12]. For example, Rotkiewicz showed that under certain hypotheses, the equation $P_p = px^2$ has no solutions (p, x) with p a prime number and x a positive integer. More precisely, his result in this direction is as follows. Here, as well as throughout the paper, we use $\left(\frac{A}{B}\right)$ to denote the Jacobi symbol of A with respect to B, where A and B are coprime integers.

2000 *Mathematics Subject Classification*: 11D25, 11B39.

Theorem R1 (Theorem 5 in [12]). *For an odd prime p the equation $P_p = px^2$, with x an integer, has no solutions provided that one of the following two sets of assumptions is satisfied*:

1. $(L, M) \equiv (1, 0) \pmod 4$ *and* $\left(\frac{M}{L}\right) = 1$, *or*
2. $(L, M) \equiv (0, 3) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$.

Rotkiewicz proved similar results concerning the equation $P_n = x^2$, under the hypothesis that the index n is prime.

Theorem R2 (Theorem 3 in [12]). *For an odd prime p the equation $P_p = x^2$, with x an integer, has no solutions provided that one of the following sets of assumptions is satisfied*:

1. $(L, M) \equiv (3, 0) \pmod 4$ *and* $\left(\frac{M}{L}\right) = 1$, *or*
2. $(L, M) \equiv (0, 1) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$.

In the first part of this paper, we prove results similar to those in Theorems R1 and R2 for different sets of Lehmer sequences.

Theorem 1. *Let p be an odd prime.*

1. *If* $(L, M) \equiv (2, 1) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then the equation* $P_p = px^2$, *with x an integer, has no solutions.*

2. *If* $(L, M) \equiv (2, 1) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then the equation* $P_p = x^2$, *with x an integer, has no solutions provided* $p > 3$.

I.1. *Diophantine applications.* Theorem 1 was motivated by certain Diophantine problems, which we will now describe. The first application of Theorem 1 concerns Diophantine equations of the form

$$mX^2 - nY^4 = c, \qquad \text{where } c \in \{1, 2, 4\}, \tag{1.2}$$

and m and n are given positive integers. Equations of the form (1.2) have been widely studied, most notably by Ljunggren in [8], wherein the following is one of the theorems proved.

Theorem L1. *If m and n are odd positive integers, then the equation*

$$mX^2 - nY^4 = 2 \tag{1.3}$$

has at most two solutions in positive integers (X, Y).

A closer look at Ljunggren's proof shows that a much more precise result can be formulated. Assume that m and n are odd positive integers for which the equation

$$mX^2 - nY^2 = 2 \tag{1.4}$$

is solvable in positive integers (X,Y). Let (a_1,b_1) be the minimal positive solution of equation (1.4), and define

$$\alpha=\frac{a_1\sqrt{m}+b_1\sqrt{n}}{\sqrt{2}}. \tag{1.5}$$

Furthermore, for k odd, define

$$\alpha^k=\frac{a_k\sqrt{m}+b_k\sqrt{n}}{\sqrt{2}}, \tag{1.6}$$

where (a_k,b_k) are positive integers. It is well known that all positive integer solutions (X,Y) of equation (1.4) are of the form (a_k,b_k). Thus, we see that a solution to (1.3) is equivalent to the existence of an index k for which $b_k=x^2$. The following is a more precise formulation of what Ljunggren actually proved.

Theorem L2. *Let m and n be odd positive integers for which* (1.4) *is solvable, and let $\alpha=(a_1\sqrt{m}+b_1\sqrt{n})/\sqrt{2}$ be the minimal solution to* (1.4). *If $b_1=v^2l$ for some squarefree integer l, then the equation $b_k=x^2$ implies that either $k=l$ or $k=3l$.*

As an application of Theorem 1, we prove the following refinement of Theorem L2. In particular, it states that the only possible value for l which can lead to solutions of (1.3) is $l=1$.

Theorem 2. 1. *If b_1 is not a square, then equation* (1.3) *has no solutions.*

2. *If b_1 is a square and b_3 is not a square, then $(X,Y)=(a_1,\sqrt{b_1})$ is the only solution of equation* (1.3).

3. *If b_1 and b_3 are both squares, then $(X,Y)=(a_1,\sqrt{b_1})$ and $(a_3,\sqrt{b_3})$ are the only solutions of equation* (1.3).

Remark. In the case that $c=1$ in equation (1.2), Ljunggren proved a result which is similar to Theorem L1. Assume that m, n are positive integers, with m not a square, such that the Pell equation

$$mX^2-nY^2=1 \tag{1.7}$$

has a positive integer solution (X,Y) and let (a_1,b_1) be the smallest such. Let

$$\alpha=a_1\sqrt{m}+b_1\sqrt{n}.$$

If $k\geq 1$ is an odd integer, then

$$\alpha^k=a_k\sqrt{m}+b_k\sqrt{n}$$

for some positive integers a_k and b_k, and all positive integer solutions of equation (1.7) are of the form $(X,Y)=(a_k,b_k)$ for some $k\geq 1$. Therefore, an integer solution to equation (1.2), with $c=1$, is equivalent to the existence of an odd index k for which $b_k = x^2$ for some integer x. If $b_1 = v^2 l$ with l squarefree, then similarly to Theorem L1, Ljunggren [8] showed that $b_k = x^2$ implies that $l = k$.

Conjecture. *If equation* (1.2) *with* $c = 1$ *is solvable*, *then* $l \le 5$.

The constant 5 above is suggested by the *abc*-conjecture. The second author (see [15]) has found parametric families (m, n) for which the equation $mX^2 - nY^4 = 1$ has a positive integer solution with $l = 3$ and also with $l = 5$.

Another Diophantine application is related to the equation

$$(X^2 - 1)(Y^2 - 1) = (Z^2 - 1)^2, \tag{1.8}$$

which according to [5] has yet to be completely solved. Schinzel and Sierpiński [13] found all the solutions of equation (1.8) when $Y - X = 2Z$, Chao Zen Fu [1] found all solutions of equation (1.8) when $Y - X = kZ$ where k is an integer with $|k| < 31$ and Luca [9] found all solutions of (1.8) when $Z \mid (Y^2 - X^2)$. While we could not succeed in solving equation (1.8) completely, we employ Theorem 1 together with Theorems R1 and R2 to solve the following variants.

Theorem 3. 1. *The equation*

$$(X^2 + 1)(Y^2 + 1) = Z^4 \tag{1.9}$$

has no positive integer solutions.

2. *The only positive integer solutions of the equation*

$$(X^2 + 1)(Y^2 - 1) = Z^4 \tag{1.10}$$

are $(X, Y, Z) = (1, 3, 1)$ *and* $(239, 3, 26)$.

3. *The equation*

$$(X^2 - 1)(Y^2 - 1) = Z^4 \tag{1.11}$$

has no positive integer solutions.

II. Preliminary results. In [12], Rotkiewicz computed formulae for $\left(\frac{P_n}{P_m}\right)$, in terms of other Jacobi symbols, which involve only the indices m and n, but are independent of the defining parameters L and M. In order to state Rotkiewicz's results, we exhibit the following sequence of equalities, according to Eisenstein's modified version of the Euclidean algorithm (see [14], p. 330):

$$
(2.1)\qquad \begin{cases}
n = 2k_1 m + \varepsilon_1 r_1, & 0 < r_1 < p,\\
m = 2k_2 r_1 + \varepsilon_2 r_2, & 0 < r_2 < r_1,\\
r_1 = 2k_3 r_2 + \varepsilon_3 r_3, & 0 < r_3 < r_2,\\
\vdots & \\
r_{l-3} = 2k_{l-1} r_{l-2} + \varepsilon_{l-1} r_{l-1}, & 0 < r_{l-1} < r_l,\\
r_{l-2} = 2k_l r_{l-1} + \varepsilon_l r_l, & r_l = 1,\\
\varepsilon_i = \pm 1, \qquad 2 \nmid r_i & \text{for } i = 1, 2, \ldots,\ l.
\end{cases}
$$

Then (see [14], p. 332), the following formula holds:

$$
(2.2)\qquad \left(\frac{n}{m}\right) = (-1)^{\sum_{i=1}^{l} \frac{r_{i-1}-1}{2}\cdot\frac{\varepsilon_i r_i - 1}{2}}, \qquad r_0 = m.
$$

With the above notations, Rotkiewicz proved the following result.

Lemma R1 (Theorem 2 in [12]).

$$
\left(\frac{P_n}{P_m}\right) = \begin{cases}
\left(\frac{n}{m}\right) & \textit{if } (L, M) \equiv (0, 1) \pmod 4,\ \left(\frac{L}{M}\right) = 1,\\
1 & \textit{if } (L, M) \equiv (0, -1) \pmod 4,\ \left(\frac{L}{M}\right) = 1,\\
\left(\frac{n}{m}\right) & \textit{if } (L, M) \equiv (-1, 0) \pmod 4,\ \left(\frac{M}{L}\right) = 1,\\
1 & \textit{if } (L, M) \equiv (1, 0) \pmod 4,\ \left(\frac{M}{L}\right) = 1,\\
(-1)^{\sum_{i=1}^{l} \frac{\left(\frac{-2}{r_{i-1}}\right)-1}{2}\cdot\frac{\varepsilon_i\left(\frac{-2}{r_i}\right)-1}{2}} & \\
 & \textit{if } (L, M) \equiv (2, 1) \pmod 4,\ \left(\frac{L}{M}\right) = 1,\ r_0 = m,\\
(-1)^{(s+\varepsilon_l-1)/2} = (-1)^{\lambda} & \\
 & \textit{if } (L, M) \equiv (1, 2) \pmod 4,\ \left(\frac{M}{L}\right) = 1,
\end{cases}
$$

where s is the number of positive ε_i's in the sequence $\varepsilon_1, \ldots, \varepsilon_{l-1}$ defined by (2.1), *and λ is the number of terms in the expansion $n/m = [a_1, \ldots, a_\lambda]$ into a simple continued fraction with $a_\lambda > 1$.*

III. Proof of Theorem 1

1. We first consider the equation $P_p = px^2$, where p is an odd prime and x is a positive integer. By equation (23) in [12], we have

$$
(3.1)\qquad P_n = (\alpha - \beta)^2 \lambda_n + n M^{(n-1)/2} \qquad \text{for all odd } n > 0,
$$

where λ_n is some rational integer. Since $P_p = px^2$, it follows that $p \mid P_p$. By a result of Lehmer (see [6]), we have $p \mid (\alpha - \beta)^2$. Now let q be any odd integer. By (3.1), and the fact that $p \mid (\alpha-\beta)^2$, it follows that

$$P_q \equiv qM^{(q-1)/2} \pmod{p}.$$

We therefore deduce the following sequence of equalities of Jacobi symbols:

$$\begin{aligned}(3.2)\quad \left(\frac{P_q}{P_p}\right) &= \left(\frac{P_q}{px^2}\right) = \left(\frac{P_q}{p}\right) = \left(\frac{qM^{(q-1)/2}}{p}\right)\\ &= \left(\frac{q}{p}\right)\cdot\left(\frac{M^{(q-1)/2}}{p}\right) = \left(\frac{q}{p}\right)\cdot\left(\frac{M^{(q-1)/2}}{P_p}\right) = \left(\frac{q}{p}\right).\end{aligned}$$

For the last equality of (3.2), we have used Lemma 3 in [12]. Thus, we have shown that the equation $P_p = px^2$ implies that

$$(3.3)\qquad \left(\frac{q}{p}\right) = \left(\frac{P_q}{P_p}\right) \qquad \text{for all odd } q > 0.$$

We note that by Lemma 1 of [12], we can restrict to the cases $p \equiv \pm 1 \pmod 8$. In what follows, we investigate the relation (3.3). Combining (2.2) and Lemma R1, we see that (3.3) is equivalent to

$$(3.4)\qquad \sum_{i=1}^{l} \frac{r_{i-1}-1}{2}\cdot\frac{\varepsilon_i r_i - 1}{2} \equiv \sum_{i=1}^{l} \frac{\left(\frac{-2}{r_{i-1}}\right)-1}{2}\cdot\frac{\varepsilon_i\left(\frac{-2}{r_i}\right)-1}{2} \pmod{2}.$$

Moreover, (3.4) holds for all odd q, where r_i and ε_i are determined in terms of q and p by the algorithm in (3.1). The proof of the first part of Theorem 1 is achieved by showing that given a prime $p \equiv \pm 1 \pmod 8$, there is some other odd integer q for which (3.4) fails to hold. For this, let us take a closer look at (3.4). Since both sums occurring in (3.4) are relevant only modulo 2, it suffices to count how many terms from each of the two sums are odd. Notice that the term

$$\frac{r_{i-1}-1}{2}\cdot\frac{\varepsilon_i r_i - 1}{2}$$

is odd if and only if $r_{i-1} \equiv \varepsilon_i r_i \equiv -1 \pmod 4$. Notice also that the term

$$\frac{\left(\frac{-2}{r_{i-1}}\right)-1}{2}\cdot\frac{\varepsilon_i\left(\frac{-2}{r_i}\right)-1}{2}$$

is odd if and only if both r_{i-1} and $\varepsilon_i r_i$ are congruent to -1 or -3 modulo 8. For the sake of brevity, we introduce the following notations:

$$\begin{aligned}\lambda_4(p,q) &= \#\{i \mid r_{i-1} \equiv \varepsilon_i r_i \equiv 3 \pmod 4\},\\ \lambda_8(p,q) &= \#\{i \mid r_{i-1} \equiv 5 \text{ or } 7 \pmod 8 \text{ and } \varepsilon_i r_i \equiv 5 \text{ or } 7 \pmod 8\}.\end{aligned}$$

With these notations, equality (3.4) is equivalent to

$$\lambda_4(p,q) \equiv \lambda_8(p,q) \pmod 2 \tag{3.5}$$

for all odd $q > 1$. The final contradiction is achieved by proving that

Claim 1. *For all prime numbers $p \equiv \pm 1 \pmod 8$ there exists an odd positive integer q such that $\lambda_4(p,q) \not\equiv \lambda_8(p,q) \pmod 2$.*

As a convention, we always write only λ_4 and λ_8 and omit the symbols p and q. Also, we will always assume that $q = 2p + r_1$, for then the choice of q will be determined from the choice of r_1.

Case 1: $p \equiv 1 \pmod 8$.

Claim 1.1. $p \equiv 1 \pmod 9$.

We first show that $p \equiv 1 \pmod 3$. If not, then the division $p = 2k \cdot 3 - 1$ has $\lambda_4 = 1$ and $\lambda_8 = 0$, contradicting (3.5). If $p \not\equiv 1 \pmod 9$, then $p \equiv -5$ or $7 \pmod{18}$. Choose $r_1 = 9$, then for $p \equiv -5 \pmod{18}$ we have

$$p = 2k \cdot 9 - 5, \qquad 9 = 2 \cdot 5 - 1,$$

which contradicts (3.5) since $\lambda_4 = 0$ and $\lambda_8 = 1$. For $p \equiv 7 \pmod{18}$, this division has $\lambda_4 = 2$ and $\lambda_8 = 1$, again violating (3.5). Therefore, $p \equiv 1 \pmod 9$, proving Claim 1.1.

Claim 1.2. $p \equiv 1$ or $2 \pmod 5$.

We choose $r_1 = 5$. If $p \equiv -1 \pmod{10}$, the division $p = 2k \cdot 5 - 1$ has $\lambda_4 = 0$ and $\lambda_8 = 1$, which contradicts (3.5). Similarly, if $p \equiv 3 \pmod{10}$ this is also in violation of (3.5), since $\lambda_4 = 1$ and $\lambda_8 = 0$. Therefore, $p \equiv 1$ or $2 \pmod 5$, which proves Claim 1.2.

From here on, we distinguish two cases.

Case 1.1: $p \equiv 1 \pmod 5$. In this case we obtain a contradiction by proving by induction that the proposition

$$P(k): \quad 3^k \mid (p-1)$$

holds for all positive integers k. Notice that $P(1)$ and $P(2)$ hold by the fact that $p \equiv 1 \pmod 9$. Assume first that $P(2k-1)$ holds. If $P(2k)$ does not hold, then $p \equiv 2 \cdot 3^{2k-1} + 1$ or $-(2 \cdot 3^{2k-1} - 1) \pmod{2 \cdot 3^{2k}}$. In both cases, we choose $r_1 = 3^{2k}$. If $p \equiv 2 \cdot 3^{2k-1} + 1 \pmod{2 \cdot 3^{2k}}$, then the resulting division has $\lambda_4 = 2$ and $\lambda_8 = 1$, which contradicts (3.5). If $p \equiv -(2 \cdot 3^{2k-1} - 1) \pmod{2 \cdot 3^{2k}}$, then the same value of r_1 yields a division in which $\lambda_4 = 0$ and $\lambda_8 = 1$, once again contradicting (3.5). The above arguments show that $P(2k-1) \Rightarrow P(2k)$.

Assume now that $P(2k)$ holds for some $k \geq 1$, but that $P(2k+1)$ does not hold. We then have $p \equiv 2 \cdot 3^{2k} + 1$ or $-(2 \cdot 3^{2k} - 1) \pmod{2 \cdot 3^{2k+1}}$. Since $p \equiv 1 \pmod 5$, it follows that $p \equiv 2 \cdot 5 \cdot 3^{2k} + 1$ or $-(2 \cdot 5 \cdot 3^{2k} - 1) \pmod{2 \cdot 5 \cdot 3^{2k+1}}$. We choose $r_1 = 5 \cdot 3^{2k+1}$. If $p \equiv 2 \cdot 5 \cdot 3^{2k} + 1 \pmod{2 \cdot 5 \cdot 3^{2k+1}}$, then r_1 gives a division with $\lambda_4 = 2$ and $\lambda_8 = 1$, which violates (3.5). If $p \equiv -(2 \cdot 5 \cdot 3^{2k} - 1) \pmod{2 \cdot 5 \cdot 3^{2k+1}}$, then r_1 yields a division with $\lambda_4 = 2$ and $\lambda_8 = 1$, once again violating (3.5). Therefore $P(2k) \Rightarrow P(2k+1)$, and so $P(k)$ holds for all $k \geq 1$, a contradiction.

Case 1.2: $p \equiv 2 \pmod 5$. Note that since $p \equiv 1 \pmod 9$, we have in this case $p \equiv -8 \pmod{5 \cdot 9}$. We use induction to prove that the proposition

$$P(k): \quad 3^k \mid (p+8),$$

holds for all $k \geq 1$. It has already been proved that $P(1)$ and $P(2)$ hold. Assume first that $P(2k-1)$ holds for some $k \geq 1$ but that $P(2k)$ does not hold. Clearly, $k \geq 2$. Since $3^{2k-1} \mid (p+8)$ and $3^{2k} \nmid (p+8)$, it follows that $p \equiv 3^{2k-1} - 8$ or $-(3^{2k-1} + 8) \pmod{2 \cdot 3^{2k}}$. We choose $r_1 = 3^{2k}$. For $p \equiv 3^{2k-1} - 8 \pmod{2 \cdot 3^{2k}}$, the resulting division has $\lambda_4 = 0$ and $\lambda_8 = 1$. If $p \equiv -(3^{2k-1} + 8) \pmod{2 \cdot 3^{2k}}$, then the resulting division has $\lambda_4 = 4$ and $\lambda_8 = 1$. As both of these violate (3.5), it follows that $P(2k-1) \Rightarrow P(2k)$.

We now show that $P(2k) \Rightarrow P(2k+1)$. Assume that this is not so and let $k \geq 1$ be such that $P(2k)$ holds but $P(2k+1)$ does not. Since $5 \cdot 3^{2k}$ divides $p+8$, but 3^{2k+1} does not divide $p+8$, it follows that $p \equiv 3^{2k} \cdot 5 - 8$ or $-(3^{2k} \cdot 5 + 8) \pmod{3^{2k+1} \cdot 5}$. In both of these cases, we choose $r_1 = 5 \cdot 3^{2k+1}$. If $p \equiv 3^{2k} \cdot 5 - 8 \pmod{3^{2k+1} \cdot 5}$, then the resulting division has $\lambda_4 = 3$ and $\lambda_8 = 2$, while if $p \equiv -(3^{2k} \cdot 5 + 8) \pmod{3^{2k+1} \cdot 5}$, then the resulting division has $\lambda_4 = 1$ and $\lambda_8 = 2$. Since both of these divisions violate (3.5), we see that $P(2k) \Rightarrow P(2k+1)$. Thus, the statement $P(k)$ is true for all $k \geq 1$, which is a contradiction. This completes the proof of Case 1.

Case 2: $p \equiv 7 \pmod 8$. The proof is very similar to the previous case. If $p \equiv 7 \pmod 8$, then arguing as in the previous case leads to $p \equiv 8 \pmod 9$, and either $p \equiv 4$ or $3 \pmod 5$. If $p \equiv 4 \pmod 5$, then one proceeds as in the previous case by proving that the proposition

$$P(k): \quad 3^k \mid (p+1),$$

holds for all $k \geq 1$. We already know that $P(1)$ and $P(2)$ hold. If $P(2k-1)$ holds, then $P(2k)$ also holds, for if not then $p \equiv 2 \cdot 3^{2k-1} - 1$ or $-(2 \cdot 3^{2k-1} + 1)$ (mod $2 \cdot 3^{2k}$), and each of these possibilities, with $r_1 = 3^{2k}$, gives a division which contradicts (3.5). For the implication $P(2k) \Rightarrow P(2k+1)$, one uses the fact that 5 divides $p+1$ to show that if $P(2k)$ holds and $P(2k+1)$ does not, then $p \equiv 2 \cdot 5 \cdot 3^{2k} - 1$ or $-(2 \cdot 5 \cdot 3^{2k} + 1)$ (mod $2 \cdot 5 \cdot 3^{2k+1}$). With $r_1 = 5 \cdot 3^{2k+1}$, both cases result in a division which violates (3.5).

Finally, if $p \equiv 7 \pmod 8$ and $p \equiv 3 \pmod 5$, then $p \equiv 8 \pmod{9 \cdot 5}$, and it can be shown by induction that the proposition

$$P(k): \quad 3^k \mid (p-8)$$

holds for all $k \geq 1$. We already know that $P(1)$ and $P(2)$ hold. If $P(2k-1)$

holds and $P(2k)$ does not, then $p \equiv 3^{2k-1} + 8$ or $-(3^{2k-1} - 8) \pmod{2 \cdot 3^{2k}}$. With $r_1 = 3^{2k}$, each of the above two possibilities gives a division violating (3.5). For the implication $P(2k) \Rightarrow P(2k+1)$, assume that $P(2k)$ holds, but that $P(2k+1)$ does not; then since 5 divides $p-8$, we have $p \equiv 5 \cdot 3^{2k} + 8$ or $-(5 \cdot 3^{2k} - 8)$ (mod $2 \cdot 3^{2k+1} \cdot 5$). Putting $r_1 = 5 \cdot 3^{2k+1}$ leads again to a division for which (3.5) fails. This completes the proof of Claim 1, and the first part of Theorem 1.

2. *The equation* $P_p = x^2$. Assume that $p > 3$. Since $P_p \equiv x^2 \equiv 1 \pmod 8$, it follows, by Lemma 1 in [12], that $p \equiv 1,\ 3 \pmod 8$. Moreover, Lemma R1 yields that

$$\sum_{i=1}^{l} \frac{\left(\frac{-2}{r_{i-1}}\right) - 1}{2} \cdot \frac{\varepsilon_i\left(\frac{-2}{r_i}\right) - 1}{2} \equiv 0 \pmod 2, \tag{3.6}$$

where q is any odd number coprime to p and the numbers ε_i, r_i for $i = 1, \dots, l$ are given by (2.1). With our previous notations, the problem is solved once we prove that:

Claim 2. *For any odd prime $p > 3$ such that $p \equiv 1,\ 3 \pmod 8$, there exists an odd number q such that $\lambda_8(p,q)$ is odd.*

We work again under the assumption that once r_1 is chosen, then q is defined as $q = 2p + r_1$. We first show that $p = \pm 1$ (mod 9). If $p \equiv \pm 5 \pmod 9$, then the division

$$p = 2k \cdot 9 \pm 5, \qquad 9 = 2 \cdot 5 - 1,$$

has $\lambda_8 = 1$, contradicting (3.5). If $p \equiv \pm 7 \pmod 9$, then the division

$$\begin{aligned} p &= 2k \cdot 9 \pm 7, \\ 9 &= 2 \cdot 7 - 5, \\ 7 &= 2 \cdot 5 - 3, \\ 5 &= 2 \cdot 3 - 1, \end{aligned}$$

also has $\lambda_8 = 1$, again contradicting (3.5), and so it follows that $p = \pm 1 \pmod 9$.

It is also easy to see that $p \equiv 1,\ 3 \pmod 5$, since each of the remaining two cases, namely $p \equiv -1,\ -3 \pmod 5$, leads to a division with $\lambda_8 = 1$.

Case 2.1: $p \equiv 1 \pmod 9$. In this case, $p \equiv 1 \pmod 5$, for if not, then $p \equiv 3 \pmod 5$, and $p \equiv 28 \pmod{45}$, and so by choosing $r_1 = 45$, we get a division with $\lambda_8 = 1$, contradicting (3.5).

We show by induction that

$$P(k): \quad 3^k \mid (p-1),$$

holds for all $k \geq 1$. In the case under consideration, we already know that $P(1)$ and $P(2)$ hold. If $P(2k-1)$ holds for some $k \geq 2$ and $P(2k)$ does not, then $p \equiv 2 \cdot 3^{2k-1} + 1$ or $-(2 \cdot 3^{2k-1} - 1) \pmod{2 \cdot 3^{2k}}$. Putting $r_1 = 3^{2k}$, we obtain in both cases a division with $\lambda_8 = 1$, contradicting (3.5). If $P(2k)$ holds for some $k \geq 1$ and $P(2k+1)$ does not, then since 5 divides $p-1$, $p \equiv 2 \cdot 5 \cdot 3^{2k} + 1$ or $-(2 \cdot 5 \cdot 3^{2k} - 1) \pmod{2 \cdot 5 \cdot 3^{2k+1}}$. If we put $r_1 = 5 \cdot 3^{2k+1}$ then either case results in a division for which $\lambda_8 = 1$, a contradiction. Thus, we have shown that $P(k)$ is true for all $k \geq 1$, which certainly cannot hold, thereby dealing with Case 2.1.

Case 2.2: $p \equiv 8 \pmod 9$. In this case, we claim that $p \equiv 3 \pmod 5$. If not, then $p \equiv 1 \pmod 5$, and therefore $p \equiv -19 \pmod{45}$. By choosing $r_1 = 45$, we obtain a division with $\lambda_8 = 3$. Hence, $p \equiv 3 \pmod 5$, and so $p \equiv 8 \pmod{45}$. We show by induction that

$$P(k): \quad 3^k \mid (p-8)$$

holds for all $k \geq 1$. In the case under consideration, we already know that $P(1)$ and $P(2)$ hold. If $P(2k-1)$ holds for some $k \geq 2$ and $P(2k)$ does not, then $p \equiv 3^{2k-1} + 8$ or $-(3^{2k-1} - 8) \pmod{2 \cdot 3^{2k}}$. Put $r_1 = 3^{2k}$; then in both cases the resulting division has $\lambda_8 = 1$. Suppose $P(2k)$ holds for some $k \geq 1$ and $P(2k+1)$ does not. Since $5 \mid (p-8)$, it follows that $p \equiv 5 \cdot 3^{2k} + 8$ or $-(5 \cdot 3^{2k} - 8) \pmod{2 \cdot 5 \cdot 3^{2k+1}}$. Put $r_1 = 5 \cdot 3^{2k+1}$; then in the first case $\lambda_8 = 3$, while in the second case $\lambda_8 = 1$. We have shown that $P(k)$ holds for all $k \geq 1$, which is impossible. This completes the proof of Claim 2, and the second part of Theorem 1.

IV. Proof of Theorem 2. Assume that $b_k = x^2$ for some odd integer $k > 1$ and some positive integer x. Let p be a prime factor of k, then $b_{k/p}$ divides b_k. Moreover, from the binomial theorem, it is easy to see that

$$\gcd(b_{k/p}, b_k/b_{k/p}) = \gcd(b_{k/p}, p) = 1 \text{ or } p. \tag{4.1}$$

Since

$$b_{k/p} \cdot \frac{b_k}{b_{k/p}} = x^2,$$

it follows from (4.1) that either $b_{k/p} = py^2$ or $b_{k/p} = y^2$ for some positive integer y. If

$$\alpha_1 = \frac{a_{k/p}\sqrt{m} + b_{k/p}\sqrt{n}}{\sqrt{2}} \quad \text{and} \quad \beta_1 = \frac{a_{k/p}\sqrt{m} - b_{k/p}\sqrt{n}}{\sqrt{2}},$$

then α_1 and β_1 are the roots of the quadratic equation

$$X^2 - \sqrt{2a_{k/p}^2 m}\, X + 1 = 0,$$

and

$$P_p = \frac{b_k}{b_{k/p}} = \frac{\alpha_1^p - \beta_1^p}{\alpha_1 - \beta_1}$$

is the pth term of the Lehmer sequence defined by $L = 2a_{k/p}^2 m$ and $M = 1$. The parameters L and M of this Lehmer sequence satisfy the hypothesis of Theorem 1, and so the equation $P_p = py^2$ is impossible, while the equation $P_p = y^2$ implies $p = 3$. Therefore, the only possibility is $b_{k/p} = y^2$ and $p = 3$. If $k \neq 3$, we can reapply the above argument to $k/3$ to get a third solution to the equation (1.3), which contradicts Theorem L1, and completes the proof of Theorem 2.

V. Proof of Theorem 3. We treat each of the three equations separately.

The equation $(X^2+1)(Y^2+1) = Z^4$*.* Define

$$\begin{aligned} R &= \{p \mid (X^2+1); \mathrm{ord}_p(X^2+1) \equiv 1 \pmod 4\},\\ S &= \{p \mid (X^2+1);\ \mathrm{ord}_p(X^2+1) \equiv 2 \pmod 4\},\\ T &= \{p \mid (X^2+1);\ \mathrm{ord}_p(X^2+1) \equiv 3 \pmod 4\}, \end{aligned}$$

and

$$r = \prod_{p \in R} p, \qquad s = \prod_{p \in S} p, \qquad t = \prod_{p \in T} p.$$

We denote by (T_1, U_1) the minimal positive solution of the equation

$$T^2 - rtU^2 = -1, \tag{5.1}$$

and for a positive integer $k \geq 1$, let (T_k, U_k) be positive integers such that

$$T_k + U_k\sqrt{rt} = (T_1 + U_1\sqrt{rt})^k.$$

It is well known that all positive solutions of equation (5.1) are of the form $(T, U) = (T_k, U_k)$ for some odd integer k. With the previous notations, it follows that $X = T_k$ and $Y = T_l$ for some odd integers k and l and that

$$U_k = rsu_1^2 \quad \text{and} \quad U_l = tsu_2^2 \tag{5.2}$$

for some positive integers u_1 and u_2. Since both k and l are odd, (5.2) implies that rt is odd as well. Let p be a prime factor of rt. Since p divides one of the numbers r or t, but not both, it follows from (5.2) and the binomial theorem, as applied in [6], that $\mathrm{ord}_p(k) \neq \mathrm{ord}_p(l)$. We assume, without loss of generality, that

$$\mathrm{ord}_p(k) > \mathrm{ord}_p(l).$$

The divisibility results in [6], together with (5.2), imply that s divides $U_{k/p}$ and $U_{k/p}$ divides U_k. Moreover,

$$U_k/U_{k/p} = pv^2 \tag{5.3}$$

for some positive integer v. If one sets

$$\alpha = T_{k/p} + U_{k/p}\sqrt{rt} \quad \text{and} \quad \beta = T_{k/p} - U_{k/p}\sqrt{rt}$$

then $U_k/U_{k/p}$ is the pth term of the Lehmer sequence whose characteristic equation has the roots α and β. This sequence satisfies the hypothesis of Theorem R1, therefore equation (5.3) is impossible, and equation (1.9) has no positive integer solutions.

The equation $(X^2+1)(Y^2-1) = Z^4$. Assume that $(X^2+1)(Y^2-1) = Z^4$. An argument similar to the one employed in the previous case shows that there exist integers k and l such that k is odd and l is even and $T_k = X$, $T_l = Y$ and

$$U_k = rsu_1^2 \quad \text{and} \quad U_l = tsu_2^2 \tag{5.4}$$

for some positive integers u_1 and u_2. Write $l = 2^a l_1$, where l_1 is odd. Since s divides U_k and k is odd, it follows that the rank of apparition of every prime divisor p of s in $\{U_n\}_{n\geq 0}$ is odd. We recall that the *rank of apparition* of a number v in the sequence $\{U_n\}_{n\geq 0}$ is the least integer $\alpha(v)$ such that $v \mid U_{\alpha(v)}$. We conclude that s is coprime to T_j for all $j \geq 1$. It now follows easily that

$$U_{l_1} = \left(\frac{t}{2^\delta}\right) su_3^2 \qquad \text{for some positive integer } u_3 \text{ and } \delta \in \{0,1\}. \tag{5.5}$$

An application of Theorem R1 similar to the one employed for the previous equation (1.9) shows that rt cannot be divisible by an odd prime. Therefore, $rt = 2$ and

$$U_k = su_1^2 \quad \text{and} \quad U_l = 2su_2^2. \tag{5.6}$$

Since s is coprime to T_j for all $j \geq 1$ and since $U_l = 2U_{l/2}T_{l/2}$, it follows, by formula (5.6), that $T_{l/2} = w^2$ for some positive integer w. Since

$$T_j^2 - 2U_j^2 = \pm 1 \qquad \text{for all } j \geq 1,$$

we see that

$$w^4 - 2U_{l/2}^2 = \pm 1.$$

A well known theorem of Ljunggren (see [8]) implies that $w = 1$ and that $l = 2$. Hence, $U_l = 2$, $s = 1$ and $U_k = u_1^2$. This last equation is equivalent to

$$T_k^2 - 2u_1^4 = -1.$$

By yet another theorem of Ljunggren (see [7]), it follows that $u_1 = 1$ or 13, which leads to the solutions $(X, Y, Z) = (1, 3, 2)$ and $(239, 3, 26)$. This completes the solution of equation (1.10).

The equation $(X^2-1)(Y^2-1) = Z^4$. We retain the definitions for r, s and t, as given at the beginning of the proof of Theorem 3, but define them to be the squarefree numbers built up from prime divisors of $X^2 - 1$ instead of X^2+1. We denote by (T_1,U_1) the minimal positive solution of the Pell equation

$$X^2 - rtY^2 = 1, \tag{5.7}$$

and let

$$\alpha = T_1 + U_1\sqrt{rt}. \tag{5.8}$$

For a positive integer $k \geq 1$, let (T_k,U_k) be positive integers given by

$$T_k + U_k\sqrt{rt} = \alpha^k.$$

Proceeding as before, it follows that there exist integers k and l such that $X = T_k,\ Y = T_l$,

$$U_k = rsu_1^2 \quad \text{and} \quad U_l = tsu_2^2. \tag{5.9}$$

We note that $\alpha = \tau^2$, where

$$\tau = \frac{a\sqrt{m}+b\sqrt{n}}{\sqrt{c}}, \tag{5.10}$$

where $a,\ b,\ c,\ m$ and n are positive integers with $mn = rt$, $c \in \{1,2\}$ and

$$a^2m - b^2n = c. \tag{5.11}$$

Moreover, from the minimality of the solution (T_1,U_1), it follows that $m > 1$ if $c = 1$.

If i is an odd positive integer, then

$$\tau^i = \frac{a_i\sqrt{m}+b_i\sqrt{n}}{\sqrt{c}} \tag{5.12}$$

for some positive integers a_i and b_i. Since $T_i + U_i\sqrt{rt} = \alpha^i = (\tau^i)^2$, it follows that $U_i = a_ib_i$ for all odd integers $i \geq 1$. At this stage we distinguish two subcases.

Case 1: $c = 1$. Write $k = 2^gk_1$ and $l = 2^hl_1$, with k_1 and l_1 odd. Then it follows that

$$U_{k_1} = (r/2^\gamma)s'v_1^2, \qquad U_{l_1} = (t/2^\delta)s'v_2^2 \tag{5.13}$$

for some positive integers v_1, v_2 and $\gamma, \delta \in \{0,1\}$, and where

$$s' = \prod_{\substack{p\mid s \\ \alpha(p) \text{ is odd}}} p.$$

Using the notations (5.10)–(5.12), (5.13) implies that

$$a_{k_1} = r_1s_1w_1^2, \qquad b_{k_1} = r_2s_2z_1^2 \qquad (r_1r_2 = r \text{ or } r/2,\ s_1s_2 = s') \tag{5.14}$$

and

$$a_{l_1} = t_1s_1w_2^2, \qquad b_{l_1} = t_2s_2z_2^2 \qquad (t_1t_2 = t \text{ or } t/2,\ s_1s_2 = s'). \tag{5.15}$$

Moreover, since

$$\gcd(r_1, n) = \gcd(t_1, n) = \gcd(r_2, m) = \gcd(t_2, m) = 1, \tag{5.16}$$

and

$$mn = rt, \tag{5.17}$$

it follows from (5.14)–(5.17) that

$$r_1 t_1 = m \text{ or } m/2,$$

and

$$r_2 t_2 = n \text{ or } n/2.$$

An argument similar to the one employed earlier in the solution of equation (1.9), employing Theorem R1 shows that neither r_1 nor t_1 can be divisible by an odd prime. Hence, $m = 2$. Since rt is even but $\gcd(r,t) = 1$, (5.9) implies that $\mathrm{ord}_2(U_k) \neq \mathrm{ord}_2(U_l)$. Therefore, from the divisibility properties of solutions to Pell's equation, we have $\mathrm{ord}_2(k) \neq \mathrm{ord}_2(l)$. We will assume without any loss of generality that $\mathrm{ord}_2(k) > \mathrm{ord}_2(l)$. Then from Lehmer's work [6], s divides $U_{k/2}$ and

$$U_{k/2} = (r/2)su_3^2 \text{ or } 2rsu_3^2, \tag{5.18}$$

for some positive integer u_3. The relation $U_k = 2T_{k/2}U_{k/2}$ and (5.18) imply that $T_{k/2} = v_3^2$ for some positive integer v_3. We get the equation

$$v_3^4 - rtU_{k/2}^2 = 1.$$

By a theorem of Cohn (see [4]), the only possibilities are $k = 2$ or $k = 4$. Hence, either T_1 or T_2 is a square. Since $m = 2$, we see that

$$\begin{aligned} \tau &= a\sqrt{2} + b\sqrt{n}, \\ \tau^2 &= (4a^2 - 1) + (2ab)\sqrt{2n} = T_1 + U_1\sqrt{rt}, \\ \tau^4 &= 2(4a^2 - 1)^2 - 1 + (4ab(4a^2 - 1))\sqrt{2n} = T_2 + U_2\sqrt{rt}. \end{aligned}$$

The equation $4a^2 - 1 = v_3^2$ obviously has no integer solutions. Also, the equation $2(4a^2 - 1)^2 - 1 = v_3^2$ has no integer solutions since -1 is a quadratic non-residue modulo $4a^2 - 1$. This concludes the analysis for the case $c = 1$.

Case 2: $c = 2$. We keep the previous notations. In this case, similar arguments to the ones employed earlier lead to the equations

$$U_{k_1} = rs'v_1^2, \qquad U_{l_1} = ts'v_2^2, \tag{5.19}$$

$$\begin{aligned} a_{k_1} &= r_1 s_1 w_1^2, \quad a_{l_1} = t_1 s_1 z_1^2 \quad (r_1 t_1 = m), \\ b_{k_1} &= r_2 s_2 w_2^2, \quad b_{l_1} = t_2 s_2 z_2^2 \quad (r_2 t_2 = n \text{ and } s_1 s_2 = s'). \end{aligned} \tag{5.20}$$

We first show that $n = 1$. Assume that this is not so and let $p \geq 3$ be a prime divisor of n. From

$$\gcd(r_2, t_2) = \gcd(r_2, s_2) = \gcd(s_2, t_2) = 1,$$

it follows that $\operatorname{ord}_p(k_1) \neq \operatorname{ord}_p(l_1)$. We assume that $\operatorname{ord}_p(k_1) > \operatorname{ord}_p(l_1)$. It follows, by Lehmer's work [6], that $s_2 \mid b_{k_1/p}$ and that

$$b_{k_1/p} = (r_2/p)s_2 v_3^2 \text{ or } pr_2 s_2 v_3^2, \tag{5.21}$$

for some positive integer v_3. Hence,

$$b_{k_1}/b_{k_1/p} = pw_3^2 \tag{5.22}$$

for some positive integer w_3. Again, using an argument employed earlier one can show that $b_{k_1}/b_{k_1/p}$ is the pth term of a Lehmer sequence satisfying the hypothesis of Theorem 1. Now Theorem 1 guarantees that equation (5.22) is impossible. Hence, $n = 1$. We now show that $m = 3$. Indeed, since $n = 1$ it follows that $m > 1$. Let p be a prime divisor of m. Since $\operatorname{ord}_p(a_{k_1}) \neq \operatorname{ord}_p(a_{l_1})$, it follows that $\operatorname{ord}_p(k_1) \neq \operatorname{ord}_p(l_1)$ either. We assume that $\operatorname{ord}_p(k_1) > \operatorname{ord}_p(l_1)$. It now follows that $b_{k_1/p} \mid b_{k_1}$, that $\gcd(p, b_{k_1}) = 1$ and that

$$b_{k_1}/b_{k_1/p} = w_4^2,$$

for some positive integer w_4. Since $b_{k_1}/b_{k_1/p}$ is the pth term of a Lehmer sequence satisfying the hypothesis of Theorem 1, it follows that $p = 3$. Hence, $m = 3$. Going back to the original problem it follows that, up to possibly interchanging k and l, the equations (5.9) are

$$U_k = 3su_1^2 \quad \text{and} \quad U_l = su_2^2, \tag{5.23}$$

where

$$T_1 + U_1\sqrt{rt} = 2 + \sqrt{3}.$$

We assume, without lost of generality, that $\operatorname{ord}_3(k) > \operatorname{ord}_3(l)$. In this case, equations (5.23) imply that $U_{k/3} = sw_5^2$ for some positive integer w_5, so

$$3(u_1/w_5)^2 = U_k/U_{k/3} = 4T_{k/3}^2 - 1 = 12U_{k/3}^2 + 3$$

or, after dividing both sides by 3 and denoting u_1/w_5 by w_6,

$$w_6^2 = (2U_{k/3})^2 + 1,$$

which is certainly impossible. This concludes the analysis for the case $c = 2$ and the proof of Theorem 3.

Acknowledgements. This work was done when the first author visited the Mathematical Institute of the Czech Academy of Sciences. He would like to thank the people of this Institute and especially Dr. Michal Křížek for their warm hospitality. The second author gratefully acknowledges NSERC grant # 2560150.

References

[1] Z. F. Chao, *A generalization of the Schinzel–Sierpiński system of equations*, J. Harbin Inst. Tech. 23 (1991), 9–14.

[2] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. 39 (1964), 537–540.

[3] —, *Squares in some recurrent sequences*, Pacific J. Math. 41 (1972), 631–646.

[4] —, *The diophantine equation* $x^4 - Dy^2 = 1$, Acta Arith. 78 (1997), 401–403.

[5] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 1994.

[6] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), 419–438.

[7] W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo 5 (1942), 1–27.

[8] —, *Ein Satz über die diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, in: 12. Skand. Mat.-Kongr. Lund 1953 (1954), 188–194.

[9] F. Luca, *A generalization of the Schinzel–Sierpiński system of equations*, Bull. Math. Soc. Sci. Math. R. S. Roumanie (N.S.) 41 (89) (1998), 181–195.

[10] W. L. McDaniel and P. Ribenboim, *Square-classes in Lucas sequences having odd parameters*, J. Number Theory 73 (1998), 14–27.

[11] —, —, *Squares in Lucas sequences having an even first parameter*, Colloq. Math. 78 (1998), 29–34.

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

[13] A. Schinzel et W. Sierpiński, *Sur l'équation diophantienne* $(x^2 - 1)(y^2 - 1) = ((\frac{y-x}{2})^2 - 1)^2$, Elem. Math. 18 (1963), 132–133.

[14] W. Sierpiński, *Elementary Theory of Numbers*, Warszawa, 1964.

[15] P. G. Walsh, *A note on Ljunggren's theorem about the Diophantine equation* $aX^2 - bY^4 = 1$, C. R. Math. Rep. Acad. Sci. Canada 20 (1998), 113–119.

Mathematical Institute UNAM
Campus Morelia
Ap. Postal 61-3 (Xangari), CP 58 089
Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

Department of Mathematics
University of Ottawa
585 King Edward Street
Ottawa, Ontario, Canada
K1N-6N5
E-mail: gwalsh@mathstat.uottawa.ca

Received on 14.3.2000
and in revised form on 25.1.2001 (3775)