ACTA ARITHMETICA
127.1 (2007)

Square-classes in Lehmer sequences having odd parameters and their applications

by

JIAGUI LUO (Haikou) and PINGZHI YUAN (Guangzhou)

1. Introduction. Let A and B be coprime positive integers and let $\square$ denote the square of an integer. There have been many papers investigating the positive integer solutions of the Diophantine equations

$$Ax^2 - By^4 = \pm 1, \pm 2, \pm 4. \tag{1}$$

Thanks to Ljunggren, we know the exact number of positive integer solutions (x, y) of the equation $Ax^2 - By^4 = 1, 2, 4$. In fact, let A, B be positive integers and $C = 1, 2, 4$, such that AB is odd if C is even; A square-free and AB not a perfect square; and let $C = 2$ when $A = 1$. Further, only such values of A, B, C are considered for which $Ax^2 - By^2 = C$ has a solution, $(x, y) = (a, b)$ being the minimal positive integer solution. Ljunggren [9] proved that:

THEOREM L1. *If* $3+4Bb^2/C$ *is not a perfect square, then* $Ax^2 - By^4 = C$ *has at most one solution in positive integers* (x, y). *The equation* $Ax^2 - By^4 = 4$ *has at most one solution in positive relatively prime integers* (x, y).

Let A and B be odd positive integers such that the Diophantine equation $Ax^2 - By^2 = 4$ has solutions in odd positive integers. Let a_1, b_1 be the minimal positive integer solution. Define

$$\frac{a_n\sqrt{A} + b_n\sqrt{B}}{2} = \left(\frac{a_1\sqrt{A} + b_1\sqrt{B}}{2}\right)^n. \tag{2}$$

With these assumptions, Ljunggren [10] proved the following two theorems:

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

Key words and phrases: recurring sequences of second order, square Lehmer numbers, Jacobi symbol, Diophantine equation.

The first author was supported by Guangdong Provincial PHD Science Foundation (no. 04300595), Hainan Provincial Natural Science Foundation (no. 80550) and NSF of China (no. 10571180).

The second author was supported by NSF of China (no. 10571180) and Guangdong Provincial Natural Science Foundation (no. 04009801).

THEOREM L2. *The Diophantine equation $Ax^4 - By^2 = 4$ has at most two solutions in positive integers x, y.*

(i) *If $a_1 = h^2$ and $Aa_1^2 - 3 = k^2$, there are only two solutions, namely, $x = \sqrt{a_1} = h$ and $x = \sqrt{a_3} = hk$.*
(ii) *If $a_1 = h^2$ and $Aa_1^2 - 3 \neq k^2$, then $x = \sqrt{a_1} = h$ is the only solution.*
(iii) *If $a_1 = 5h^2$ and $A^2a_1^4 - 5Aa_1^2 + 5 = 5k^2$, then the only solution is $x = \sqrt{a_5} = 5hk$.*

Otherwise there are no solutions.

THEOREM L3. *The Diophantine equation $Ax^4 - By^2 = 1$ has at most one solution in positive integers x, y. If $x = x_1$, $y = y_1$ is a solution, then $x_1^2A^{1/2} + y_1B^{1/2} = \left(\frac{1}{2}(a_1A^{1/2} + b_1B^{1/2})\right)^3$.*

Let m and n be odd positive integers and suppose that (a_1, b_1) is the minimal positive integer solution of $mX^2 - nY^2 = 2$. Define

$$\frac{a_k\sqrt{m} + b_k\sqrt{n}}{\sqrt{2}} = \left(\frac{a_1\sqrt{m} + b_1\sqrt{n}}{\sqrt{2}}\right)^k. \tag{3}$$

Luca and Walsh [11] showed:

THEOREM LW.

(i) *If b_1 is not a square, then the equation*

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

has no solutions (X, Y).

(ii) *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 (4).*
(iii) *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 (4).*

However, a similar result for the equation $Ax^2 - By^4 = 4$ has not been obtained yet.

For the results of this section, it will be assumed that A and B are odd positive integers such that the Diophantine equation

$$Ax^2 - By^2 = 4 \tag{5}$$

is solvable in odd integers x and y. This assumption will be referred to as *Hypothesis* $(\star)$. Let (x_1, y_1) be the minimal positive integer solution of (5), and define

$$\frac{x_n\sqrt{A} + y_n\sqrt{B}}{2} = \left(\frac{x_1\sqrt{A} + y_1\sqrt{B}}{2}\right)^n. \tag{6}$$

We will obtain:

THEOREM 1.1. *Assume that Hypothesis* ($\star$) *holds.*

(i) *If* y_1 *is not a square, then the equation*

$$Ax^2 - By^4 = 4 \tag{7}$$

has no positive integer solutions except for the case $y_1 = 3\square$ *and* $By_1^2 + 3 = 3\square$, *when* $(x, y) = (x_3, \sqrt{y_3})$ *is the only solution of* (7).

(ii) *If* y_1 *is a square, then* (7) *has at most one positive integer solution other than* $(x, y) = (x_1, \sqrt{y_1})$, *which is either* $(x, y) = (x_3, \sqrt{y_3})$ *or* $(x, y) = (x_2, \sqrt{y_2})$, *the latter occurring if and only if* x_1 *and* y_1 *are both squares and* $A = 1$, $B \neq 5$.

THEOREM 1.2. *Assume that Hypothesis* ($\star$) *holds. Then the equation*

$$Ax^2 - By^4 = 1 \tag{8}$$

has at most one positive integer solution. The only possible solution (x, y) *is given by* $y = \sqrt{y_3/2} = hk$, *where* $y_1 = h^2, P_3 = 2k^2$.

COROLLARY 1.1. *Assume that Hypothesis* ($\star$) *holds. Then equation* (8) *has a positive integer solution if and only if* $y_1 = \square$, $y_3 = y_1 P_3 = 2\square$.

Let $R > 0$ and Q be nonzero coprime integers with $R - 4Q > 0$. Let α and β be the two roots of the trinomial $x^2 - \sqrt{R}\,x + Q$. The *Lehmer sequence* $\{P_n(R, Q)\}$ and the *associated Lehmer sequence* $\{Q_n(R, Q)\}$ with parameters R and Q are defined as follows:

$$P_n = P_n(R, Q) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & 2 \nmid n, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & 2 \mid n, \end{cases} \tag{9}$$

$$Q_n = Q_n(R, Q) = \begin{cases} (\alpha^n + \beta^n)/(\alpha + \beta), & 2 \nmid n, \\ \alpha^n + \beta^n, & 2 \mid n. \end{cases} \tag{10}$$

Note that $P_n(1, -1)$ and $Q_n(1, -1)$ are the Fibonacci numbers and Lucas numbers. It is easy to see that $P_n, Q_n \in \mathbb{Z}$ for all positive integers n.

We say that the terms P_n and P_m are *in the same square-class* if their product is a square. A square-class containing at least one element of the Lehmer sequence is called nontrivial. For a Lehmer sequence, an important problem is to decide whether it contains nontrivial classes or not, and then to find all elements in a nontrivial class. Obviously, the problem is equivalent to finding all n such that $P_n = k\square$, where k is a given integer.

Recently, many special cases of this type of problem have been considered. We recall the relevant known facts:

(a) Cohn [4], Alfred [1], Burr [3], Wyler [19] and Ko and Sun [8] showed that $P_n = 144$ is the only square Fibonacci number greater than 1.

(b) Ljunggren [9] determined, for all odd positive integers R and $Q = 1$, all indices n such that $Q_n(R, Q)$ or $nQ_n(R, Q)$ is a square.

(c) Cohn [5]–[7], determined the squares and double squares in $\{P_n\}_{n=1}^{\infty}$ and $\{Q_n\}_{n=1}^{\infty}$ when $R = P^2$ is odd or some special even integer and $Q = \pm 1$.

(d) In his seminal paper [17], Rotkiewicz partly solved the problem for R and Q with $2 \mid RQ$.

(e) In [13], [14] and [16], McDaniel and Ribenboim found all positive integers m and n such that $P_m P_n = \square$ or $Q_m Q_n = \square$ with $1 \le m < n$, $n \ne 3m$ when both $R = P^2$ and Q are odd integers. Moreover, if $P_m P_n = \square$ or $Q_m Q_n = \square$ and $n = 3m$, they proved that there exists an effectively computable constant C satisfying $m < C$. See Theorems 1 through 4 in [14] for details.

Observe that $Q_m(R, x), Q_m(x, Q) \in \mathbb{Z}[x]$, and both polynomials have only simple roots. Hence by Theorems 9.2 and 10.6 of [18], for given R, Q, k, k_1, if

$$Q_m(R, Q) Q_{km}(R, Q) = k_1 y^r, \tag{11}$$

then $\max(m, r) < C_1$, where C_1 is an effectively computable constant depending only on R, Q, k, k_1; if equation (3) holds for given m, R, k, k_1 or m, Q, k, k_1, then $\max(Q, r)$ (or $\max(P, r)$) $< C_2$, where C_2 is an effectively computable constant depending only on m, R (or Q), k and k_1. Therefore, the effective results in [13], [14], [16] are special cases of the above remark. However, the size of the computable constants—were it computed—would often be too large to enable finding all the solutions.

In [21], the second author proved the following

Proposition 1.1. *Let R and Q be coprime odd integers with $D = R - 4Q > 0$. If $Q_n = \square$ or $n\square$, then $n = 1, 3, 5$.*

In the present paper, we will prove

Proposition 1.2. *For a given integer k, let d_0 be the first index d with $k \mid Q_d$. If $Q_d = k\square$ or $2k\square$, then $d = d_0 d_1$ and $d_1 = 1, 3, 5$.*

Proposition 1.3. *If $Q_n = k\square$, $k \mid n$, then $n = 1, 3, 5$. If $Q_n = 2k\square$, $k \mid n$, then $n = 3$.*

2. Preliminaries. We first list the properties which will be used. For easy reference, we note that $P_2 = 1$, $P_3 = R - Q$, $Q_2 = R - 2Q$, $Q_3 = R - 3Q$. Most of the properties below may be proved directly. For details, we refer to the book of Ribenboim [15] and the paper of the second author [20]. Unless otherwise stated, m and n are arbitrary integers. For simplicity, in this paper we denote $(\alpha^{dr} + \beta^{dr})/(\alpha^d + \beta^d)$ and $(\alpha^r + \beta^r)/(\alpha + \beta)$ by $Q_{r,d}$ and Q_r respectively.

Proposition 2.1.

(1) *If* $3 \mid Q_d$ *with* d *odd, then* $3 \mid R$.
(2) *For odd integers* r *and* d, *we have* $\gcd(Q_{r,d}, Q_d) \mid r$.
(3) *If* p *is an odd prime with* $p \mid R$, *then* $p \mid Q_n$ *if and only if* n/p *is an odd integer.*
(4) P_m *is even for* $m > 0$ *if and only if* $3 \mid m$.
(5) Q_m *is even for* $m > 0$ *if and only if* $3 \mid m$.
(6) *If* $d = \gcd(m, n)$, *then* $\gcd(P_m, P_n) = P_d$.
(7) *If* $d = \gcd(m, n)$, *then* $\gcd(Q_m, Q_n) = V_d$ *if* m/d *and* n/d *are odd, and* 1 *or* 2 *otherwise.*
(8) *If* $d = \gcd(m, n)$, *then* $\gcd(P_m, Q_n) = Q_d$ *if* m/d *is even, and* 1 *or* 2 *otherwise.*
(9) *Let* p *be an odd prime, and* $\varepsilon = (DR|p)$ *be the Kronecker symbol. If* $p \nmid RQ$, *then* $P_{p-\varepsilon} \equiv 0 \pmod{p}$.
(10) *Let* q *be a prime,* m, k *positive integers, and* α, λ *nonnegative integers with* $\gcd(q, k) = 1$ *and* $\operatorname{ord}_q(P_m) = \alpha$. *If* $q^\alpha \neq 2$, *then* $\operatorname{ord}_q(P_{kmq^\lambda}) = \alpha + \lambda$. *Here* $\operatorname{ord}_q(n)$ *denotes the rational number* t *such that* $q^t \mid n$ *but* $q^{t+1} \nmid n$.
(11) *If* $n \geq 1$, *then* $\gcd(P_n, Q) = \gcd(Q_n, Q) = 1$.
(12) $V_m^2 - DU_m^2 = 4Q^m$, *where* $V_m = \alpha^m + \beta^m, U_m = (\alpha^m - \beta^m)/(\alpha - \beta)$.
(13) *Let* p *be an odd prime. If* $p^2 \mid D$, *then* $\operatorname{ord}_p(P_n) = \operatorname{ord}_p(n)$.

The following two lemmas are Lemmas 1, 2(a) and 4(I) of [20].

Lemma 2.1. *Let* $j = 2^u g$, $2 \nmid g$, $g > 0$, *and let* $0 \leq m \leq j$. *Then, if* $0 \leq v < u$,

(i) $Q_{2j+m} \equiv -Q^j Q_m \pmod{V_{2^u}}$ *and* $Q_{2j+m} \equiv Q^j Q_m \pmod{V_{2^v}}$,
(ii) $Q_{2j-m} \equiv -Q^{j-m} Q_m \pmod{V_{2^u}}$ *and* $Q_{2j-m} \equiv Q^{j-m} Q_m \pmod{V_{2^v}}$.

Lemma 2.2. *Let* $u \geq 2$ *be an integer. Then*

(i) $V_{2^u} \equiv -1 \pmod{8}$,
(ii) $(Q_3 | V_{2^u}) = 1$.

Lemma 2.3.

(i) *If* p *is a positive integer with* $p \mid R$ *and* $p \equiv 3 \pmod{8}$, *then* $(p|V_4) = 1$.
(ii) *If* a *is a positive integer with* $a \mid (R - 3Q) = Q_3$, *then* $(a|V_4) = 1$.

Proof. (i) By the assumption and Lemma 2.2(i),

$$(p|V_4) = -(V_4|p) = -((R - 2Q)^2 - 2Q^2|p) = -(2Q^2|p) = 1.$$

(ii) Lemma 2.2(i) again yields $(2|V_4) = 1$. Thus it suffices to prove the assertion for a odd. In fact,

$$(a|V_4) = (-1)^{(a-1)/2}(V_4|a) = (-1)^{(a-1)/2}(-Q^2|a) = 1. \blacksquare$$

Lemma 2.4. *Let p, d and a be positive integers satisfying*

$$d \equiv \pm 3 \pmod 8, \quad p \equiv 3 \pmod{16}, \quad (a|V_4) = 1.$$

Then

$$Q_d Q_{pd} \neq a\Box.$$

Proof. Suppose $Q_d Q_{pd} = a\Box$. By assumption, we can write

$p = 16k+3$, $d = 2j+m$, $j = 2^u g$, $2 \nmid g$, $u \geq 2$ and $m = -3$ or $m = -5$.

First we consider the case $m = -3$. Note that $pd = 2(pj - 24k - 4) - 1$. If $u = 2$, then by Lemma 2.1 we obtain

$$Q_d \equiv -Q^{j-3} Q_3 \pmod{V_4}, \quad Q_{pd} \equiv Q^{pj-24k-5} \pmod{V_4};$$

if $u > 2$, then

$$Q_d \equiv Q^{j-3} Q_3 \pmod{V_4}, \quad Q_{pd} \equiv -Q^{pj-24k-5} \pmod{V_4}.$$

This yields

$$1 = (a|V_4) = (Q_d Q_{pd}|V_4) = (-Q_3|V_4) = -1,$$

a contradiction.

Next we consider the case $m = -5$. Similarly, $pd = 2(pj - 40k - 8) + 1$. If $u = 2$, by Lemma 2.1 again

$$Q_d \equiv -Q^{j-5} Q_5 \pmod{V_4}, \quad Q_{pd} \equiv -Q^{pj-40k-8} \pmod{V_4};$$

if $u > 2$, then

$$Q_d \equiv Q^{j-5} Q_5 \pmod{V_4}, \quad Q_{pd} \equiv Q^{pj-40k-8} \pmod{V_4}.$$

This yields

$$1 = (a|V_4) = (Q_d Q_{pd}|V_4) = (QQ_5|V_4) = (Q(V_4 - QQ_3)|V_4) = -1,$$

again a contradiction. ∎

Combining Lemmas 2.3 and 2.4 we obtain the following two corollaries.

Corollary 2.1. *Let p and d be positive integers such that $p \mid R$, $p \equiv 3 \pmod{16}$ and $d \equiv \pm 3 \pmod 8$. Then $Q_d Q_{pd} \neq \Box, p\Box$. In particular,*

$$Q_d Q_{3d} \neq \Box, 2\Box, 3\Box, 6\Box$$

when $3 \mid R$ and $d \equiv \pm 3 \pmod 8$.

Corollary 2.2. *Let a, p and d be positive integers such that $a \mid (R - 3Q)$, $p \equiv 3 \pmod{16}$ and $d \equiv \pm 3 \pmod 8$. Then $Q_d Q_{pd} \neq \Box, a\Box$.*

Corollary 2.3. *Let d be an odd positive integer and k a positive integer with $k \mid Q_d$. If p is a positive integer such that $p \equiv \pm 3 \pmod 8$ and $p \mid (R - 3Q)$, then $Q_{3pd} \neq kr\Box$ with $r \mid 6p$. In particular, if $5 \mid (R - 3Q)$, then*

$$Q_{15d} \neq k\Box, 2k\Box, 3k\Box, 5k\Box, 6k\Box, 10k\Box, 15k\Box, 30k\Box.$$

Proof. Suppose $Q_{3pd} = kr\square$ and $r \mid 6p$. Then $Q_{3pd} = Q_{pd}Q_{3,pd} = kr\square$. Since $\gcd(Q_{pd}, Q_{3,pd}) \mid 3$ and $k \mid Q_{pd}$, it follows that $Q_{pd} = kr_1\square$, $r_1 \mid 6p$, and so

$$Q_{pd}Q_{3pd} = a\square, \qquad a \mid 6p, \tag{12}$$

and $(a|V_4) = 1$ by Lemmas 2.2 and 2.3. If $d \equiv \pm 1$, then $pd \equiv \pm 3 \pmod 8$, and so (5) is impossible by Lemma 2.4. Now we assume that $d \equiv \pm 3 \pmod 8$. Since $Q_{3pd} = Q_dQ_{3p,d} = kr\square$, $r \mid 6p$, we then have $Q_d = kr_2\square$, $r_2 \mid 3p$. Similarly, $Q_{3d} = kr_3\square$, $r_3 \mid 3p$. Therefore

$$Q_dQ_{3d} = b\square, \qquad b \mid 3p,$$

which is impossible by Lemmas 2.3 and 2.4. ∎

LEMMA 2.5. *Let d be an odd positive integer and k a positive integer with $k \mid Q_d$. Then $Q_{15d} \neq k\square, 2k\square$.*

Proof. If $Q_{15d} = k\square$, then $Q_{5d}Q_{3,5d} = k\square$. Since $\gcd(Q_{3,5d}, Q_{5d}) \mid 3$, we have $Q_{5d} = k\square$ or $3k\square$, whence

$$Q_{5d}Q_{15d} = \square \text{ or } 3\square,$$

which is impossible if $d \equiv \pm 1 \pmod 8$ by Lemmas 2.3 and 2.4. Similarly, $Q_{3d} = k\square$ or $3k\square$ is impossible if $d \equiv \pm 3 \pmod 8$.

By Corollary 2.3 and the above arguments, we may assume that $d \equiv \pm 3 \pmod 8$, $5 \nmid (R-3Q)$ and $Q_{3d} \neq k\square, 3k\square$. Since $Q_{15d} = Q_{5,3d}Q_{3d} = k\square$ and $\gcd(Q_{3d}, Q_{5,3d}) \mid 5$, we have

$$Q_{3d} = 5k\square,$$

which implies that either $5 \mid R$ or $5 \mid P_{5-\varepsilon}$, where $\varepsilon = (DR|5)$ is the Kronecker symbol. If $\varepsilon = 1$, then $5 \mid P_4$. It follows that $5 \mid \gcd(P_4, Q_{3d}) = Q_1 = 1$ by Proposition 2.1(8), a contradiction. If $\varepsilon = -1$, then $5 \mid P_6$. It follows that $5 \mid \gcd(P_6, Q_{3d}) = Q_3 = R-3Q$, which contradicts $5 \nmid (R-3Q)$. If $\varepsilon = 0$, then $5 \mid D$. Since $V_{3d}^2 - DU_{3d}^2 = 4Q^m$, it follows that $5 \mid Q$, which is impossible by Proposition 2.1(11). Hence we get $5 \mid R$ and $5 \mid d$. Now $Q_{3d} = Q_{3,d}Q_d = 5k\square$ and $\gcd(Q_d, Q_{3,d}) \mid 3$, hence $Q_d = 5k\square$ or $15k\square$, and so

$$Q_dQ_{3d} = \square \text{ or } 3\square,$$

contrary to Corollary 2.1. The proof of $Q_{15d} \neq 2k\square$ goes in exactly the same way. ∎

3. Proofs of propositions

Proof of Proposition 1.2. Put $d_0 = 3^{s_0}d_0'$, $d = 3^s d'$, $3 \nmid d_0'd'$. Then $s \geq s_0$ and $d_0' \mid d'$. By Proposition 2.1(2),(3) we have

$$\gcd(Q_{d'}, Q_{3^s,d'}) \mid 3^s, \qquad 3 \nmid Q_{d'}.$$

Thus

$$\gcd(Q_{d'}, Q_{3^s,d'}) = 1.$$

Similarly,

(13) $$\gcd(Q_{d_0'}, Q_{3^{s_0},d_0'}) = 1.$$

By Proposition 2.1(6),

(14) $$\gcd(Q_{d'/d_0',d_0'}, Q_{3^{s_0},d_0'}) = 1.$$

From $Q_{d'} = Q_{d_0'} Q_{d'/d_0',d_0'}$, (13) and (14), we have

(15) $$\gcd(Q_{d'}, Q_{3^{s_0},d_0'}) = 1.$$

Let

(16) $$\gcd(k, Q_{d_0'}) = k_1, \quad \gcd(k, Q_{3^{s_0},d_0'}) = k_2.$$

Then from $k \mid Q_{d_0} = Q_{d_0'} Q_{3^{s_0},d_0'}$ and (6), we have

(17) $$\gcd(k_1, k_2) = 1, \quad k = k_1 k_2.$$

By hypothesis, we have

(18) $$Q_{3^s d'} = Q_{d'} Q_{3^s,d'} = k_1 k_2 \square.$$

It follows from (15)–(18) that

(19) $$Q_{d'} = k_1 \square.$$

Write $r = d'/d_0'$. Then by (19), we get

$$Q_{d_0'} Q_{r,d_0'} = k_1 \square.$$

Since $k_1 \mid Q_{d_0'}$ and $\gcd(Q_{r,d_0'}, Q_{d_0'}) \mid r$, we obtain

$$Q_{r,d_0'} = r_1 \square, \quad r_1 \mid r.$$

Let $r = r_1 r_2$. Then the above equality becomes

$$Q_{r_1,r_2 d_0'} Q_{r_2,d_0'} = r_1 \square.$$

It follows that

(20) $$Q_{r_2,d_0'} = \square, \quad Q_{r_1,r_2 d_0'} = r_1 \square.$$

Since $\gcd(Q_{r_1,r_2 d_0'}/r_1, Q_{r_2 d_0'}) = 1$ and $Q_{r_2 d_0'} = Q_{r_2,d_0'} Q_{d_0'}$, by Proposition 1.1 we get $r_1 = 1, 5$ and $r_2 = 1, 5$. The case of $r_1 = r_2 = 5$ is impossible since then $5 \mid R$, and so $5 \parallel Q_{5,d_0'}$, which contradicts the first equality of (20).

If $s \geq s_0 + 2$, then $Q_{3,3^{s-1}d'} Q_{3^{s-1}d'} = k\square$ and $k \mid Q_{3^{s-1}d'}$, and so

(21) $$Q_{3^{s-1}d'} = k\square \text{ or } 3k\square.$$

In exactly the same way, we have

(22) $$Q_{3^{s-2}d'} = k\square \text{ or } 3k\square.$$

Therefore

(23) $$Q_{3^s d'} Q_{3^{s-1}d'} = \square \text{ or } 3\square$$

and

$$Q_{3^{s-1}d'}Q_{3^{s-2}d'} = \square \text{ or } 3\square. \tag{24}$$

Since $3^{s-1}d' \equiv \pm 3 \pmod 8$ or $3^{s-2}d' \equiv \pm 3 \pmod 8$, one of the equalities (23) and (24) is impossible by Lemma 2.4. Thus we conclude that $s \le s_0 + 1$ and $r = 1$ or 5, and so $d = d_0, 3d_0, 5d_0$ or $15d_0$. However, $d = 15d_0$ is impossible by Lemma 2.5. The case of $Q_d = 2k\square$ is similar, which proves Proposition 1.2.

Proof of Proposition 1.3. Similarly, we only prove the case $Q_n = k\square$, the proof for $Q_n = 2k\square$ being similar. Without loss of generality we may assume that k is square-free. Let $n/k = t$. Then

$$Q_{k,t}Q_t = k\square. \tag{25}$$

Let p be a prime divisor of k. Then p is odd and $p \mid Q_t(\alpha)R$. By Proposition 2.1(9) it follows that $\mathrm{ord}_p(Q_{k,t}) \ge \mathrm{ord}_p(k)$. Therefore, by the arbitrary choice of p and the assumption that k is square-free, we infer that $k \mid Q_{k,t}$, say $Q_{k,t} = km$. We first claim that $\gcd(m, Q_t) = 1$. Otherwise there is a prime $p \mid m$ with $p \mid Q_t$, and by Proposition 2.1(9) again, $\mathrm{ord}_p(Q_{k,t}) = \mathrm{ord}_p(k)$ contradicting $\mathrm{ord}_p(Q_{k,t}) = \mathrm{ord}_p(k) + \mathrm{ord}_p(m) > \mathrm{ord}_p(k)$. Combining this with (25) we get

$$Q_{k,t} = k\square, \qquad Q_t = \square. \tag{26}$$

From $Q_t = \square$ and Proposition 1.1 we get $t = 1, 3$ or 5. If $t = 1$ or 5, from $Q_{k,t} = k\square$ and Proposition 1.1 again we get $k = 1, 3$ or 5. However, $k = t = 5$ leads to the equation $Q_{25} = 5\square$, which is impossible by considering the 5-parts of both sides. Thus we have proved that if $Q_n = k\square$, $k \mid n$ and $3 \nmid n$, then $n = 1$ or 5. We will use this fact in the following argument when $t = 3$.

Suppose that $t = 3$. Then $Q_{3k} = k\square$. If $3 \mid k$, say $k = 3k'$, $3 \nmid k'$, then

$$Q_{9,k'}Q_{k'} = 3k'\square.$$

Since $\gcd(Q_{9,k'}, Q_{k'}) \mid 9$ and $3 \nmid Q_{k'}$, we get

$$Q_{k'} = k_1\square, \qquad k_1 \mid k', \tag{27}$$

and it follows that $k' = 1$ or 5 as above. If $3 \nmid k$, then similarly we have $k = 1$ or 5.

Combining the above arguments, to prove the theorem, it suffices to prove that the following equations are impossible:

$$Q_9 = 3\square, \qquad Q_{15} = 5\square,$$
$$Q_{15} = 3\square, \qquad Q_{45} = 15\square.$$

By Corollary 2.1, it is easy to prove that $Q_9 = 3\square$ and $Q_{15} = 3\square$ are impossible. From $Q_{45} = 15\square$ we get $Q_{15} = 5\square$. Therefore we are only left with the equation $Q_{15} = 5\square$, which implies that either $5 \mid (R-3Q)$ or $5 \mid R$ by Proposition 2.1(8),(9). However, it is impossible when $5 \mid (R-3Q)$ by Corollary 2.3 and it is impossible when $5 \mid R$ by Corollary 2.1. We are done.

4. Proofs of theorems. To prove the above theorems, we need Proposition 1.3 and some results of Ribenboim and McDaniel [16].

Let $P > 1$ be an odd integer, $\alpha = (P+\sqrt{P^2-4})/2$, $\beta = (P-\sqrt{P^2-4})/2$,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n = \alpha^n + \beta^n, \qquad n = 1, 2, \ldots.$$

Then by Theorems 1 and 2 of [16] (note that $Q = 1$), we have

LEMMA 4.1.
(i) *If* $V_n = \square$, *then* $n = 1$.
(ii) *If* $V_n = 2\square$, *then* $n = 3$.

LEMMA 4.2 ([12]). *If* $A > 1$, *then all positive integer solutions* (x, y) *of the equation* (5) *are of the form* (x_n, y_n) *with* $2 \nmid n$, *where* (x_n, y_n) *is defined by* (6). *If* $A = 1$, *then all positive integer solutions* (x, y) *of* (5) *are of the form* (x_n, y_n).

LEMMA 4.3 ([22]). *If* $\varepsilon = x_1\sqrt{A} + y_1\sqrt{B}$ *is the minimal positive integer solution of* (5), *then* $a\sqrt{A} + b\sqrt{B} = (\varepsilon/2)^3$ *is the minimal positive integer solution of the equation*

$$Ax^2 - By^2 = 1.$$

LEMMA 4.4 ([2]). *The only positive integer solutions of the Diophantine equation*

$$3x^4 - 2y^2 = 1$$

are $(x, y) = (1, 1)$ *and* $(3, 11)$.

Proof of Theorem 1.1. First we consider the case of y_1 not a square. Let

$$\alpha = \frac{x_1\sqrt{A} + y_1\sqrt{B}}{2}, \qquad \overline{\alpha} = \frac{x_1\sqrt{A} - y_1\sqrt{B}}{2}.$$

Suppose that (x, y) is a positive integer solution of (7). By Lemma 4.2,

$$\frac{x\sqrt{A} + y^2\sqrt{B}}{2} = \left(\frac{x_1\sqrt{A} + y_1\sqrt{B}}{2}\right)^n \tag{28}$$

for some positive integer $n > 1$. Thus

$$y^2 = y_1 P_n \tag{29}$$

where $P_n = (\alpha^n - \overline{\alpha}^n)/(\alpha - \overline{\alpha})$. Let d be the square-free part of y_1. From (29) we have

$$P_n = d\square, \qquad d \mid y_1. \tag{30}$$

Since $D = (\alpha - \overline{\alpha})^2 = By_1^2$, we have $d \mid n$ by Proposition 2.1(13). If n is an odd, then we obtain $n = 3$ or 5 by (30) and Proposition 1.3.

When $n = 3$, we have $d = 3$. Hence $y_1 = 3\square$ and

$$\begin{aligned} P_3 &= (\alpha^3 - \overline{\alpha}^3)/(\alpha - \overline{\alpha}) = \alpha^2 + \alpha\overline{\alpha} + \overline{\alpha}^2 \\ &= (\alpha + \overline{\alpha})^2 - \alpha\overline{\alpha} = Ax_1^2 - 1 = By_1^2 + 3 = 3\square, \end{aligned}$$

and so $y^2 = y_1 P_3 = y_3$.

When $n = 5$, we have $d = 5$. Then $y_1 = 5u^2$ and

$$\begin{aligned} P_5 &= \frac{\alpha^5 - \overline{\alpha}^5}{\alpha - \overline{\alpha}} = \alpha^4 + \alpha^3\overline{\alpha} + \alpha^2\overline{\alpha}^2 + \alpha\overline{\alpha}^3 + \overline{\alpha}^4 \\ &= ((\alpha + \overline{\alpha})^2 - 2)^2 + (\alpha + \overline{\alpha})^2 - 3 = (Ax_1^2 - 2)^2 + Ax_1^2 - 3 \\ &= (By_1^2 + 2)^2 + By_1^2 + 1 = B^2 y_1^4 + 5By_1^2 + 5 = 5v^2. \end{aligned}$$

Hence $625B^2u^4 + 125Bu^2 + 5 = 5v^2$. Completing the square and simplifying the result yields the equation $(2v)^2 - 5(10Bu^2 + 1)^2 = -1$, which implies that $(2v, 10Bu^2 + 1)$ is a solution of the Pell equation

$$x^2 - 5y^2 = -1. \tag{31}$$

Since $2 + \sqrt{5}$ is the fundamental solution of (31), we have

$$2v + (10Bu^2 + 1)\sqrt{5} = (2 + \sqrt{5})^n \tag{32}$$

for some odd integer $n > 1$. Thus

$$10Bu^2 + 1 = \sum_{r=0}^{(n-1)/2} \binom{n}{2r+1} 2^{(n-2r-1)/2} 5^r, \tag{33}$$

which implies that $10Bu^2 + 1$ is congruent to $1 \pmod 4$ and hence that B is even, contrary to assumption.

If n is even, say $n = 2m$, it follows that $A = 1$ by Lemma 4.2. By (30), we get

$$P_m V_m = d\square,$$

where $V_m = \alpha^m + \overline{\alpha}^m$. By Proposition 2.1(8),(13), $\gcd(P_m, V_m) = 1$ or 2 and $d \mid P_m$, and so

$$P_m = d\square,\ V_m = \square, \quad \text{or} \quad P_m = 2d\square,\ V_m = 2\square. \tag{34}$$

Assume the latter; then $m = 3$ by Lemma 4.1, and so $d = 3$, $y_1 = 3\square$. Noticing that $x_1^2 - By_1^2 = 4$, we get $x_1^2 \equiv 4 \pmod 9$. Since $P_3 = (\alpha + \overline{\alpha})^2 - \alpha\overline{\alpha} = x_1^2 - 1 = 6\square$, it follows that $3 \equiv 6\square \pmod 9$, so $1 \equiv 2\square \pmod 3$, which is impossible. Now we consider the former equalities of (34). By Lemma 4.1 again, $m = 1$, so $d = 1$, which contradicts the assumption that y_1 is not a square. This proves (i).

Suppose now that y_1 is a square. Let $(x, y) \neq (x_1, \sqrt{y_1})$ be another solution of (7). We also have equation (30) with $d = 1$. If n is odd, similarly we get $n = 3$ or 5. Now we are in a position to prove that the case of $n = 5$ is impossible. Otherwise write $P_5 = h^2$. Then $P_5 = B^2y_1^4 + 5By_1^2 + 5 = h^2$, and so $(2By_1^2+5)^2-5 = (2h)^2$, which is impossible. Hence $n = 3, y^2 = y_1P_3 = y_3$.

If n is even, then $A = 1$ by Lemma 4.2. Write $n = 2m$. By (30), we get

$$P_mV_m = \square.$$

By Proposition 2.1(8),(13), $\gcd(P_m, V_m) = 1$ or 2 and $d \mid P_m$. Therefore we have

$$P_m = \square,\ V_m = \square, \quad \text{or} \quad P_m = 2\square,\ V_m = 2\square. \tag{35}$$

In the former case, we have $m = 1$ by Lemma 4.1. It follows that $y^2 = y_2 = y_1P_2 = x_1y_1$, which implies that $x_1 = \square$, $y_1 = \square$.

From the latter equalities of (35), we have $m = 3$ by Lemma 4.1. Since $P_3 = x_1^2 - 1 = 2\square$, $V_3 = x_1(x_1^2 - 3) = 2\square$, we have either

$$x_1 = 3h^2, \quad x_1^2 - 3 = 6k^2, \quad \gcd(x_1, x_1^2 - 3) = 3, \tag{36}$$

or

$$x_1 = \square, \quad x_1^2 - 3 = 2\square, \quad \gcd(x_1, x_1^2 - 3) = 1. \tag{37}$$

(37) implies that $1 \equiv 2 \pmod 3$, a contradiction. From (36), we conclude that $3h^4 - 2k^2 = 1$, and so $(h, k) = (1, 1)$ or $(3, 11)$ by Lemma 4.4.

When $(h, k) = (1, 1)$, $x_1 = 3$, $P_3 = x_1^2 - 1 = 8$, $V_3 = x_1(x_1^2 - 3) = 18$, we have $P_6 = P_3V_3 = 12^2, By_1^2 = x_1^2 - 4 = 5$, which implies that $B = 5$, $y_1 = 1$. Thus $y = \sqrt{y_1P_6} = 12$.

When $(h, k) = (3, 11)$, $x_1 = 27$, a simple computation shows that $x_1^2-1 = 728 \neq 2\square$, which contradicts $P_3 = x_1^2 - 1 = 2\square$.

This completes the proof.

Proof of Theorem 1.2. Let

$$\alpha = \frac{x_1\sqrt{A} + y_1\sqrt{B}}{2}, \quad \overline{\alpha} = \frac{x_1\sqrt{A} - y_1\sqrt{B}}{2}.$$

By Lemma 4.3, $\varepsilon = \alpha^3$ is the minimal positive integer solution of the equation $Ax^2 - By^2 = 1$. Assume that (x, y) is a positive integer solution of (5). Then

$$x\sqrt{A} + y^2\sqrt{B} = \varepsilon^n \tag{38}$$

for some positive integer n. Thus

$$2y^2 = y_1P_{3n}. \tag{39}$$

Let d be the square-free part of y_1. From (39) we have

$$P_{3n} = 2d\square, \quad d \mid y_1. \tag{40}$$

Similarly, since $D = (\alpha-\overline{\alpha})^2 = By_1^2$, we have $d \mid 3n$. If n is odd, we obtain $n = 1$ by (40) and Proposition 1.3. Hence $d = 1$ or 3. If $d = 3$, then $y_1 = 3\square$.

Since $Ax_1^2 - By_1^2 = 4$, we obtain $Ax_1^2 \equiv 4 \pmod 9$. From $P_3 = Ax_1^2 - 1 = 6\square$, it is easy to see that $3 \equiv 6\square \pmod 9$. Thus $1 \equiv 2\square \pmod 3$, which is impossible. So $d = 1$, $y_1 = h^2$, $P_3 = 2k^2$, $2y^2 = y_1 P_3 = y_3 = 2h^2k^2$. Thus $y = \sqrt{y_3/2} = hk$.

If n is even, say $n = 2m$, then $A = 1$. By (40), we get

$$P_{3m} V_{3m} = 2d\square.$$

By Proposition 2.1(4),(5),(8),(13), $\gcd(P_{3m}, V_{3m}) = 2$ and $d \mid P_{3m}$. Therefore we have either

$$P_{3m} = 2d\square, \qquad V_{3m} = \square, \tag{41}$$

which is impossible by Lemma 4.1, or

$$P_{3m} = d\square, \qquad V_{3m} = 2\square. \tag{42}$$

By Lemma 4.1, we obtain $m = 1$ from the latter equality of (42). By the former equality of (42) we get $d = 1$ or 3. Then $P_3 = x_1^2 - 1 = \square$ or $3\square$, and it follows that $3 \nmid x_1$. It is easy to prove that $\gcd(x_1, x_1^2 - 3) = 1$. Thus from $V_3 = x_1(x_1^2 - 3) = 2\square$ and $2 \nmid x_1$, we deduce that $x_1^2 - 3 = 2\square$, which implies that $1 = (2|3) = -1$, a contradiction. This completes the proof.

Corollary 1.1 is an immediate consequence of Theorem 1.2.

Acknowledgements. The authors are grateful to the referees for their valuable suggestions.

References

[1] U. Alfred, *On square Lucas numbers*, Fibonacci Quart. 2 (1964), 11–12.

[2] R. T. Bumby, *The diophantine equation* $3x^4 - 2y^2 = 1$, Math. Scand. 21 (1967), 144–148.

[3] S. A. Burr, *On the occurrence of squares in Lucas sequences*, Notices Amer. Math. Soc. (Abstract 63T-203), 10 (1963), 367.

[4] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. 39 (1964), 537–541.

[5] —, *Eight diophantine equations*, Proc. London Math. Soc. 16 (1966), 153–166.

[6] —, *Five diophantine equations*, Math. Scand. 21 (1967), 61–70.

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

[8] C. Ko and Q. Sun, *On square Fibonacci numbers*, J. Sichuan Univ. 11 (1965), 11–18 (in Chinese).

[9] W. Ljunggren, *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.

[10] —, *On the diophantine equation* $Ax^4 - By^2 = C$ ($C = 1, 4$), Math. Scand. 21 (1967), 149–158.

[11] F. Luca and P. G. Walsh, *Squares in Lehmer sequences and some Diophantine applications*, Acta Arith. 100 (2001), 47–62.

[12] J. G. Luo, *Extensions and applications on Störmer's theory*, J. Sichuan Univ. 28 (1991), 469–474 (in Chinese).

[13] W. L. McDaniel, *Square Lehmer numbers*, Colloq. Math. 66 (1993), 85–93.
[14] W. L. McDaniel and P. Ribenboim, *Square-classes in Lucas sequences having odd parameters*, J. Number Theory 73 (1998), 14–27.
[15] P. Ribenboim, *The Book of Prime Number Records*, Springer, New York, 1989.
[16] P. Ribenboim and W. L. McDaniel, *The square terms in Lucas sequences*, J. Number Theory 58 (1996), 104–123.
[17] A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, Acta Arith. 42 (1983), 163–187.
[18] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, Cambridge, 1986.
[19] O. Wyler, *Solution of problem 5080*, Amer. Math. Monthly 71 (1964), 220–222.
[20] P. Z. Yuan, *A note on the divisibility of the generalized Lucas' sequences*, Fibonacci Quart. 40 (2002), 153–156.
[21] —, *The square terms in Lehmer sequences*, Acta Math. Sinica 46 (2003), 897–902 (in Chinese).
[22] P. Z. Yuan and J. G. Luo, *On solutions of higher degree diophantine equation*, J. Math. Res. Expo. 21 (2001), 99–102 (in Chinese).

Department of Applied Mathematics
College of Information Science and Technology
Hainan University
Haikou, 570228, P.R. China
E-mail: jg_luo@tom.com

Department of Mathematics
Sun Yat-sen University
Guangzhou, 510275, P.R. China
E-mail: mcsypz@zsu.edu.cn

Received on 1.4.2006
and in revised form on 8.11.2006 (5181)