INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A55

ON THE DIOPHANTINE EQUATION $X^2 + 3^m = Y^n$

Tao Liqun
Department of Mathematics, Nanjing University, Nanjing 210093, P. R. China
and
School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland
lqtao99@tom.com

Received: 2/15/08, Revised: 5/23/08, Accepted: 7/10/08, Published: 12/3/08

Abstract

In this paper we consider the diophantine equation $x^2 + 3^m = y^n, n > 2, m, n \in \mathbf{N}$. When $2 \mid m$, we determine complete solutions of the equation with the help of a deep result due to Bilu, Hanrot, and Voutier, and when $2 \nmid m$, we rewrite a proof due to E. Brown in a little different way.

1. Introduction

The diophantine equation $x^2 + k = y^n$, $x, y, n \in \mathbf{Z}$, $n > 2$ has been studied extensively. When $n = 3$, it is well known as Mordell's equation, which Mordell discussed in detail in his book [9]. When $n > 3$, there is now also a vast amount of literature. For small positive k, it seems easier to determine the solutions. For example, V. A. Lebesgue [7] proved that there are no nontrivial solutions when $k = 1$. Nagell [10] showed that there are no solutions when $k = 3$ and 5. In the case $k = 2$, Ljunggren [8] proved that the equation has only one solution $x = 5$. J. H. E. Cohn treated the equation for values of positive k under 100 and found complete solutions for 77 values, see [4]. When $k = c^m$, c a positive integer, $m \in \mathbf{N}$ unknown, the equation is more difficult to treat, even for very small c. In the case $c = 2$, on the basis of the work of Cohn [3], Le and Guo [5] found complete solutions with the aid of computers. In this paper we consider the case $c = 3$. Brown [2] has found all solutions for $2 \nmid m$, so we need only to consider the equation for $2 \mid m$. However for the sake of completeness we also give a simple proof here which is just a rewriting of [2] in a little different way. Le conjectured in [6] that the equation $x^2 + 3^{2m} = y^n, (x, y) = 1, n > 2, m, n \in \mathbf{N}$ has only one positive integer solution $(x, y, m, n) = (46, 13, 2, 3)$. Using the method E. Brown called "rough decent" [2], we show this conjecture is true in all cases except when n is a prime of the form $12k - 1$. To complete the proof we use the result in [1] to cover the exceptional case.

2. The equation $x^2 + 3^{2m+1} = y^n$

We begin by considering the general equation $x^2 + 3^m = y^n, n > 2$. If $(x, y) \neq 1$, then $3 \mid x$, $3 \mid y$. Suppose $3^s \parallel x$, $3^t \parallel y$. If $2 \nmid m$, we have $m = tn < 2s$ or $2s = tn < m$. So the equation can be written as

$$3X^2 + 1 = Y^n \tag{1}$$

or

$$X^2 + 3^{m'} = Y^n, (X, Y) = 1, 2 \nmid m' \tag{2}$$

If $2 \mid m$, then either $m = tn \leq 2s$, or $2s = tn < m$, or $2s = m < tn$. The third case is easily exclude, for then we have $X^2 + 1 = 3^{tn-m}Y^n$, hence $X^2 + 1 \equiv 0 \mod 3$, which is impossible. For the former two cases the equation can be written as

$$X^2 + 1 = Y^n \tag{3}$$

or

$$X^2 + 3^{m'} = Y^n, (X, Y) = 1, m' > 0, 2 \mid m' \tag{4}$$

Equation (3) has been treated in [7], and the equation $x^2+3 = y^n, n > 2$ has been treated in [10], so we need only consider (1), (2) for $m' > 1$ and (4). In this section we treat (1) and (2).

Throughout the paper we will use freely the fact that $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-3}]$ are unique factorization domains.

Theorem 2.1. The equation $3x^2 + 1 = y^n, n > 2$ has no positive integer solutions.

Proof. Since $n > 2$, arguing modulo 8, one obtains that if there exist integers x, y such that $3x^2 + 1 = y^n$, then y is odd and x is even. Hence the algebraic integers $1 + x\sqrt{-3}$ and $1-x\sqrt{-3}$ are coprime. If $n = 4$, there exist integers a, b such that $1+x\sqrt{-3} = \pm(a+b\sqrt{-3})^4$. Comparing the real part, we have $1 = \pm(a^4 - 18a^2b^2 + 9b^4)$. Since $3 \nmid a$, hence $a^2 \equiv 1 \mod 3$, we see the minus case is rejected. So we have $1 = (a^2 - 9b^2)^2 - 72b^4$. Consider the equation $X^2 - 72Y^4 = 1$. Suppose (x', y') is a nonnegative integer solution. Then $\frac{x'+1}{2}\frac{x'-1}{2} = 18y'^4$. So there exist integers s, t such that $y' = st$, $\frac{x'+1}{2} = 2s^4$ and $\frac{x'-1}{2} = 9t^4$, or $\frac{x'-1}{2} = 2s^4$ and $\frac{x'+1}{2} = 9t^4$, or $\frac{x'+1}{2} = 18s^4$ and $\frac{x'-1}{2} = t^4$, or $\frac{x'-1}{2} = 18s^4$ and $\frac{x'+1}{2} = t^4$. For the former two cases we have $2s^4 - 9t^4 = \pm 1$, for the latter two cases we have $18s^4 - t^4 = \pm 1$. It is easy to see that $2s^4 - 9t^4 = 1$ and $18s^4 - t^4 = 1$ are impossible by considering modulo 3.

By Lesbegue's result [7], $18s^4 - t^4 = -1$ has only one solution $(s, t) = (0, \pm 1)$. Then $y' = 0$. So $b = 0$, hence $x = 0$. (We can also solve the equation $18s^4 - t^4 = -1$ directly: we have $(t^2+1)(t^2-1) = 18s^4$. Hence $2 \mid (t^2 \pm 1)$. Moreover we have $2 \parallel (t^2+1)$, because otherwise

$t^2 \equiv 3 \mod 4$, which is impossible. Suppose that $t \neq \pm 1$. Since $(\frac{t^2+1}{2})(t^2-1) = (3s^2)^2$ and $(\frac{t^2+1}{2}, t^2-1) = 1$, there is an integer z such that $t^2 - 1 = z^2$, which implies $t = \pm 1$. This is a contradiction; therefore we have the only integer solutions $t = \pm 1, s = 0$.)

For $2s^4 - 9t^4 = -1$, we have $\frac{3t^2+1}{2}\frac{3t^2-1}{2} = 8(\frac{s}{2})^4$. Then as above we get $u^4 - 8v^4 = \pm 1$ and $uv = \frac{s}{2}$ for some integers u, v. The minus case is rejected by considering modulo 8. From [9] (see p. 208) the equation $u^4 - 8v^4 = 1$ has only one solution $(u, v) = (1, 0)$. Then we see $s = 0$, hence $3t^2 = 1$, which is impossible.

Now we may assume n is an odd prime p. Suppose (x, y, m, p) is a solution. Then there exist some integers a, b such that $1 + x\sqrt{-3} = (a + b\sqrt{-3})^p$ and $y = a^2 + 3b^2$.

Comparing the real parts, we have

$$1 = a \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k} a^{p-(2k+1)} (-3b^2)^k. \tag{5}$$

Then we see $a = \pm 1$. So from (5) we have $\pm 1 \equiv 1 \mod 3$; hence $a = 1$. Thus $\sum_{k=1}^{\frac{p-1}{2}} \binom{p}{2k}(-3b^2)^k = 0$.

Let $V_2(\cdot)$ be the standard 2-adic valuation. For $k \geq 2$, let $k = 2^s t, 2 \nmid t$. Then when $s = 0$, $2(k-1) = 2(t-1) \geq 2 > 0 = V_2(k)$; and when $s > 0$, $2(k-1) = 2(2^s t - 1) \geq 2(2^s - 1) \geq 2s > s = V_2(k)$. So $2(k-1) > V_2(k)$ for $k \geq 2$.

From $3x^2 + 1 = y^p$, we have $2 \nmid y$. As $y = a^2 + 3b^2 = 1 + 3b^2$, we see $2 \mid b$. Since $x > 0$, we have $y > 1$. So $b \neq 0$. Then for $k \geq 2$, we have

$$\begin{aligned} &V_2(\tbinom{p}{2k}(-3b^2)^k) = V_2(\tfrac{p(p-1)}{2k(2k-1)}\tbinom{p-2}{2k-2}(-3b^2)^k) \\ &= V_2(\tbinom{p}{2}(-3b^2)) + V_2(\tfrac{1}{k(2k-1)}\tbinom{p-2}{2k-2}(-3b^2)^{k-1}) \\ &\geq V_2(\tbinom{p}{2}(-3b^2)) + 2(k-1) - V_2(k) > V_2(\tbinom{p}{2}(-3b^2)). \end{aligned}$$

But from $0 = \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{2k}(-3b^2)^k$, we see there are at least two terms with smallest 2-adic valuation. This is a contradiction. This completes the proof of the theorem. □

Theorem 2.2. The equation $x^2 + 3^{2m+1} = y^n, (x, y) = 1, n > 2, m \geq 1$ has only one positive integer solution $(x, y, m, n) = (10, 7, 2, 3)$.

Proof. When $n = 4$, we have $(y^2 + x)(y^2 - x) = 3^{2m+1}$. Then $y^2 + x = 3^{2m+1}$ and $y^2 - x = 1$. So $2y^2 = 3^{2m+1} + 1$. Then $2 \equiv 2y^2 \equiv 1 \mod 3$, which is impossible.

Now we assume n is an odd prime p. Suppose (x, y, m, p) is a solution. Since $(2, y) = 1$ and $(3, y) = 1$(because $(x, y) = 1$), the algebraic integers $x \pm 3^m\sqrt{-3}$ are coprime. Then there exist some integers a, b such that $x + 3^m\sqrt{-3} = (a + b\sqrt{-3})^p$ and $y = a^2 + 3b^2$.

Comparing the imaginary parts, we have $3^m = b\sum_{k=0}^{\frac{p-1}{2}}\binom{p}{2k+1}a^{p-(2k+1)}(-3b^2)^k$, so that $b \mid 3^m$. Let $b = \pm 3^l, 0 \le l \le m$. Then $\pm 3^{m-l} = \sum_{k=0}^{\frac{p-1}{2}}\binom{p}{2k+1}a^{p-(2k+1)}(-3b^2)^k$. So $\pm 3^{m-l} \equiv pa^{p-1} \equiv p \mod 3$ (since $3 \nmid y$ implies $3 \nmid a$).

If $p = 3$, we have $\pm 3^{m-l} = 3a^2 - 3b^2$, or $\pm 3^{m-l-1} = a^2 - b^2$. If $l > 0$, then $l = m - 1$ since $3 \nmid a$, hence $\pm 1 = a^2 - b^2 \equiv a^2 \mod 3$. So the minus case is excluded and we have $1 = a^2 - b^2$. Then $a^2 = 1 + b^2 = 1 + 3^{2(m-1)} \equiv 2 \mod 8$, which is impossible. So $l = 0$, hence $b = \pm 1$. Then we have $\pm 3^{m-1} = a^2 - 1 = (a+1)(a-1)$, so $a + 1 = \pm 3^{m-1}$ and $a - 1 = \pm 1$, or $a - 1 = \pm 3^{m-1}$ and $a + 1 = \pm 1$. In both cases we have $3^{m-1} - 1 = \pm 2$, hence $m = 2$. Then we get $a = \pm 2$, so $y = 7$ and $x = 10$.

If $p \ne 3$, then $m = l$. Hence, $b = \pm 3^m$ and $p \equiv \pm 1 \mod 3$ accordingly.

Since $x^2 + 3^{2m+1} = y^p$, by considering this modulo 8 we see that $2 \nmid y$. Then from $y = a^2 + 3b^2$ and $2 \nmid b$, we have $2 \mid a$. Thus $\pm 1 = \sum_{k=0}^{\frac{p-1}{2}}\binom{p}{2k+1}a^{p-(2k+1)}(-3b^2)^k \equiv 1 \mod 4$. So $b = 3^m$ and hence $p \equiv 1 \mod 3$. This gives us $p \equiv 1 \mod 6$.

Let $N = p - 1$. Then $6 \mid N$. Suppose $3^{r+2m} \mid N$ (here we do not assume that $r \ge 0$, but we have $r + 2m > 0$. We write this way just for convenience of computation in the following), we will prove $3^{r+2m+1} \mid N$, which leads to a contradiction. So the equation $x^2 + 3^{2m+1} = y^p, (x,y) = 1, p \equiv 1 \mod 6$ has no integer solutions, thus finishing the proof of the theorem.

Let $\alpha = a + 3^m\sqrt{-3}$. Let $V_3(\cdot)$ be the standard 3-adic valuation. For $k \ge 2$, let $k = 3^s t, 3 \nmid t$. Then when $s = 0$, we have $k - 2 = t - 2 \ge 0 = V_3(k)$; and when $s > 0$, $k - 2 = 3^s t - 2 \ge 3^s - 2 \ge s = V_3(k)$. So $k - V_3(k) \ge 2$ for $k \ge 2$.

Then for $k \ge 2$, we have

$$\begin{aligned}&V_3(\tbinom{N}{k}(3^m\sqrt{-3})^k) \ge V_3(\tfrac{N}{k}(3^m\sqrt{-3})^k)) = V_3(N) - V_3(k) + (m+\tfrac{1}{2})k\\ &\ge r + 2m + (m-\tfrac{1}{2})k + (k - V_3(k)) \ge r + 2m + (m-\tfrac{1}{2})k + 2 \ge r + 4m + 1.\end{aligned}$$

So

$$\alpha^N = (a + 3^m\sqrt{-3})^N \equiv a^N + Na^{N-1}3^m\sqrt{-3} \mod 3^{r+4m+1}.$$

Thus

$$\begin{aligned}\alpha^p = \alpha\cdot\alpha^N &\equiv \alpha a^N + \alpha N a^{N-1}3^m\sqrt{-3} = \alpha a^N + (a + 3^m\sqrt{-3})Na^{N-1}3^m\sqrt{-3}\\ &= \alpha a^N + Na^N 3^m\sqrt{-3} - Na^{N-1}3^{2m+1} \equiv \alpha a^N + Na^N 3^m\sqrt{-3} \mod 3^{r+4m+1} \qquad (6)\end{aligned}$$

Since $x + 3^m\sqrt{-3} = (a + b\sqrt{-3})^p$ and $b = 3^m$, we have

$$\alpha^p - \bar{\alpha}^p = (a + 3^m\sqrt{-3})^p - (a - 3^m\sqrt{-3})^p = (x + 3^m\sqrt{-3}) - (x - 3^m\sqrt{-3}) = 2\cdot 3^m\sqrt{-3},$$

where $\bar{\alpha}$ is the complex conjugate.

Taking the conjugate of (6), and then subtracting from (6), and substituting the above equation, we get $2\cdot 3^m\sqrt{-3} = 2\cdot 3^m\sqrt{-3}a^N + 2\cdot 3^m\sqrt{-3}Na^N \mod 3^{r+4m+1}$. Thus, $3^{r+2m+1} \mid ((a^N-1)+Na^N)$. Since $3 \mid (a^2-1)$ and $V_3(\binom{\frac{N}{2}}{k}3^k) \geq V_3(N) - V_3(k) + k \geq r+2m+1$ for $k \geq 1$, from $a^N - 1 = ((a^2-1)+1)^{\frac{N}{2}} - 1 = \sum_{k=1}^{\frac{N}{2}} \binom{\frac{N}{2}}{k}(a^2-1)^k$, we have $3^{r+2m+1} \mid (a^N-1)$. Hence $3^{r+2m+1} \mid Na^N$. Therefore $3^{r+2m+1} \mid N$. This completes the proof the theorem. □

3. The Equation $x^2 + 3^{2m} = y^p,\ p \equiv 1 \mod 12$

In this section, we treat Case (4). At first we consider some simple cases.

Theorem 3.1. The equation $x^2 + 3^{2m} = y^4, (x,y) = 1$ has no positive integer solution.

Proof. Since $3 \nmid xy$, from $(y^2+x)(y^2-x) = 3^{2m}$, we have $y^2 + x = 3^{2m}$ and $y^2 - x = 1$. So $2y^2 = 3^{2m} + 1$. Thus $2 \equiv 2y^2 \equiv 1 \mod 3$, which is impossible. □

Theorem 3.2. The equation $x^2 + 3^{2m} = y^3, (x,y) = 1$ has only one positive integer solution $(x,y,m) = (46,13,2)$.

Proof. Suppose (x,y,m) is a solution. Since y is odd and $(3,y) = 1$ (because $(x,y) = 1$), we have $x + 3^m i$ and $x - 3^m i$ are coprime. Then there exist integers a, b such that $x + 3^m i = (a+bi)^3$ and $y = a^2 + b^2$. Comparing the imaginary parts we have $3^m = 3a^2b - b^3$, so $3 \mid b$.

Now let $b = \pm 3^l, l > 0$. Then $\pm 3^{m-l-1} = a^2 - 3^{2l-1}$. Since $3 \nmid y$ and $3 \mid b$, we have $3 \nmid a$. So $l = m-1$. Hence $\pm 1 = a^2 - 3^{2m-3}$. Since $a^2 \equiv 1 \mod 3$, the minus sign is rejected. So $a^2 - 1 = 3^{2m-3}$. Then $a+1 = \pm 3^{2m-3}$ and $a-1 = \pm 1$, or $a-1 = \pm 3^{2m-3}$ and $a+1 = \pm 1$. In both cases we get $3^{2m-3} - 1 = \pm 2$. So $m = 2$, hence $a = \pm 2$. Therefore we have the solution $(x,y,m) = (46,13,2)$. □

In view of the above discussion, we need only consider $x^2 + 3^{2m} = y^p, (x,y) = 1, m \geq 1$, where $p > 3$ is a prime. Suppose (x,y,m,p) is a solution. Then there exist integers a and b such that $y = a^2 + b^2$ and $x + 3^m i = (a+bi)^p$. Comparing the imaginary parts we have

$$3^m = b\sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} a^{p-(2k+1)}(-b^2)^k. \tag{7}$$

Since $3 \nmid xy$, we have $x^2 \equiv y^2 \equiv 1 \mod 3$, hence from $x^2 + 3^{2m} = y^p$, we get $y \equiv 1 \mod 3$. If $b = \pm 1$, then from $y = a^2 + b^2 = a^2 + 1 \mod 3$, we have $3 \mid a$. But from (7), we get $3^m \equiv b(-b^2)^{\frac{p-1}{2}} \mod a$, so we have $3 \mid b$. This is a contradiction. So $3 \mid b$. We may assume $b = \pm 3^l, l > 0$. Again from (7), we obtain $\pm 3^{m-l} \equiv pa^{p-1} \equiv p \mod 3$. Since $p > 3$, we get $m = l$, hence $b = \pm 3^m$. Moreover $p \equiv \pm 1 \mod 3$ according as $b = \pm 3^m$.

Accordingly, we also have

$$\pm 1 = \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} a^{p-(2k+1)}(-b^2)^k. \tag{8}$$

From (8) we have $\pm 1 \equiv (-b^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p$. Hence, $p \equiv \pm 1 \mod 4$ accordingly. Thus, $p \equiv \pm 1 \mod 12$ according as $b = \pm 3^m$.

Theorem 3.3. The equation $x^2 + 3^{2m} = y^p, (x, y) = 1,\ p \equiv 1 \mod 12$ has no integer solution.

Proof. Suppose (x, y, m, p) is a solution. Then there exist integers a, b such that $x + 3^m i = (a + bi)^p$ and $y = a^2 + b^2$. Since $p \equiv 1 \mod 12$, we have $b = 3^m$. Let $N = p - 1$ so that $3 \mid N$. Suppose $3^{r+2m} \mid N$, we will prove that $3^{r+2m+1} \mid N$, which leads to a contradiction, as desired. □

Now let $\alpha = a + 3^m i, i = \sqrt{-1}$. Recall that in last section we proved that, for $k \geq 2$, we have $k - V_3(k) \geq 2$. Since $\binom{N}{k} = \frac{N}{k}\binom{N-1}{k-1}$, we have, for $k \geq 2$,

$$V_3(\binom{N}{k}3^{mk}) \geq V_3(\frac{N}{k}3^{mk}) = V_3(N) - V_3(k) + mk \geq r + 2m + (m-1)k + 2 \geq r + 4m.$$

So $\alpha^N = (a + 3^m i)^N \equiv a^N + Na^{N-1}3^m i \mod 3^{r+4m}$. Thus,

$$\begin{aligned} \alpha^p = \alpha \cdot \alpha^N &\equiv \alpha a^N + \alpha N a^{N-1} 3^m i = \alpha a^N + (a + 3^m i) N a^{N-1} 3^m i \\ &= \alpha a^N + N a^N 3^m i - N a^{N-1} 3^{2m} \equiv \alpha a^N + N a^N 3^m i \mod 3^{r+4m}. \end{aligned} \tag{9}$$

Since $x + 3^m i = (a + bi)^p$ and $b = 3^m$, we have $\alpha^p - \bar{\alpha}^p = (a + 3^m i)^p - (a - 3^m i)^p = (x + 3^m i) - (x - 3^m i) = 2 \cdot 3^m i$, where $\bar{\alpha}$ is the complex conjugate.

Taking the conjugate of (9), and then subtracting from (9), and substituting the above equation, we get $2 \cdot 3^m i = 2 \cdot 3^m i a^N + 2 \cdot 3^m i N a^N \mod 3^{r+4m}$.

Thus, $3^{r+3m} \mid ((a^N - 1) + Na^N)$. Since $3 \mid (a^2 - 1)$ and $V_3(\binom{\frac{N}{2}}{k}3^k) \geq V_3(N) - V_3(k) + k \geq r + 2m + 1$ for $k \geq 1$, from $a^N - 1 = ((a^2 - 1) + 1)^{\frac{N}{2}} - 1 = \sum_{k=0}^{\frac{N}{2}} \binom{\frac{N}{2}}{k}(a^2 - 1)^k$, we have $3^{r+2m+1} \mid (a^N - 1)$. Hence $3^{r+2m+1} \mid Na^N$. Therefore $3^{r+2m+1} \mid N$. □

4. The Equation $x^2 + 3^{2m} = y^p,\ p \equiv -1 \mod 12$

Theorem 4.1. The equation $x^2 + 3^{2m} = y^p,\ p \equiv -1 \mod 12$ has no integer solution.

Before giving the proof, we introduce the following notions; see [1].

Definition 4.2. Let α, β be two algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ are nonzero coprime rational integers and $\frac{\alpha}{\beta}$ is not a root of unity. Then we call (α, β) a Lucas pair and define the corresponding sequence of Lucas numbers by

$$u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ n = 0, 1, 2, \ldots.$$

Definition 4.3. Let (α, β) be a Lucas pair. A prime p is a primitive divisor of $u_n(\alpha, \beta)$ if p divides u_n but does not divide $(\alpha - \beta)^2 u_1 u_2 \cdots u_{n-1}$.

Definition 4.4. A Lucas pair (α, β), such that $u_n(\alpha, \beta)$ has no primitive divisors, is called an n-defective Lucas pair. If no Lucas pair is n-defective, then n is called totally non-defective.

Lemma 4.5. ([**1**]) Every integer $n > 30$ is totally non-defective.

Proof of Theorem 4.1. Suppose (x, y, m, p) is a solution of the equation $x^2+3^{2m} = y^p, (x, y) = 1, p \equiv -1 \mod 12$. Then as before we get $x+3^m i = (a+bi)^p$ and $y = a^2+b^2$ for some integers a, b. Since $p \equiv -1 \mod 12$, we have $b = -3^m$(see the paragraph above the statement of Theorem 3.3). Let $\alpha = a+3^m i$, $\beta = a-3^m i$. Then we have $\alpha^p-\beta^p = (a+3^m i)^p - (a-3^m i)^p = (x + 3^m i) - (x - 3^m i) = -2 \cdot 3^m i = -(\alpha - \beta)$. So $u_p(\alpha, \beta) = \frac{\alpha^p - \beta^p}{\alpha - \beta} = -1$. It is obvious that (α, β) is a Lucas pair, so by Lemma 4.5 $u_p(\alpha, \beta)$ always has a primitive divisor when $p > 30$. When $p = 11$ or 23, we see from Table 1 of Theorem C in [1] that 11 and 23 are also totally non-defective, so the above argument can be applied. Thus $|u_p(\alpha, \beta)| > 1$ for a prime p of the form $12k - 1$. This is a contradiction. This completes the proof of the theorem. □

Acknowledgement. The author is very grateful to the referee for helpful suggestions.

References

[1] Yu. Bilu, G. Hanrot and P. M .Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, J. Reine Angew. Math., 539 (2001), 75-122.

[2] E. Brown, Diophantine equations of the form $ax^2 + Db^2 = y^p$, J. Reine Angew. Math., 291 (1977), 118-127.

[3] J. H. E. Cohn, The diophantine equation $x^2 + 2^k = y^n$, Arch. Math. (Basel), 59 (1992), 341-344.

[4] J. H. E. Cohn, The diophantine equation $x^2 + C = y^n$, Acta Arith., LXV. 4 (1993), 367-381.

[5] Maohua Le and Yongdong Guo, On the diophantine equation $x^2 + 2^k = y^n$, Chinese Science Bulletin, 42 (1997), 1255-1257.

[6] Maohua Le, The Applications of the Method of Gel'fond-Baker to Diophantine Equations, Science Press, Beijing, 1998.

[7] V. A. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, Nouvelles Annales des Mathématiques (1) 9 (1850), 178-181.

[8] W. Ljunggren, On the diophantine equation $x^2 + p^2 = y^n$, Norske Vid. Seisk Porh. Trondheim 16 (8) (1943), 27-30.

[9] L. J. Mordell, Diophantine Equations, Academic Press, London, 1969.

[10] T. Nagell, Sur l'impossibilité de quelques equations à deux indéterminees, Norsk. Mat. Forensings Skrifter, 13 (1923), 65-82.