On the diophantine equation $x^4 - q^4 = py^n$

Liu Yanyan

School of Education, Tibet University For Nationalities, Xianyang, Shaanxi, PR China

Received 10 April 2012; received in revised form 11 October 2012

Abstract

Let $n$, $p$ and $q$ be odd primes. In this paper, using some arithmetical properties of Lucas numbers, we prove that if $n > 3$ and $p \equiv 3 \pmod{4}$, then the equation $x^4 - q^4 = py^n$ has no positive integer solution $(x, y)$ satisfying $\gcd(x, y) = 1$ and $2 \nmid y$.

© 2013 Elsevier GmbH. All rights reserved.

MSC 2010: primary 11D41; secondary 11D61

Keywords: Higher diophantine equation; Lucas number; Arithmetical property

1. Introduction

Let $\mathbb{Z}$, $\mathbb{N}$ be the sets of all integers and positive integers respectively. Let $p$ and $q$ be odd primes. Recently, F. Luca and A. Togbé [6] have proved that the equation

$$x^4 - q^4 = py^3, \quad x, y \in \mathbb{N}, \quad \gcd(x, y) = 1,$$

(1.1)

has no solution $(x, y)$. The proof of this result used the existence of integral points on certain elliptic curves.

Let $n$ be an odd prime. In this paper we deal with a general equation

$$x^4 - q^4 = py^n, \quad x, y \in \mathbb{N}, \quad \gcd(x, y) = 1.$$

(1.2)

This equation is one of many varieties of Fermat’s equation (see [2–5,8]). Using some arithmetical properties of Lucas numbers, we prove the following result.

Theorem. If $n > 3$ and $p \equiv 3 \pmod{4}$, then (1.2) has no solution $(x, y)$ with $2 \nmid y$. 

E-mail address: yyliu1016@163.com.

0723-0869/ - see front matter © 2013 Elsevier GmbH. All rights reserved.
doi:10.1016/j.exmath.2013.01.001
2. Preliminaries

For any real number $z$, let
\[
P_n(z) = z \sum_{i=0}^{(n-1)/2} (-1)^i \binom{n}{2i} z^{n-2i-1},
\]
\[
Q_n(z) = \sum_{i=0}^{(n-1)/2} (-1)^i \binom{n}{2i+1} z^{n-2i-1}.
\quad (2.1)
\]

Lemma 2.1. If $z > 2n/\pi$, then $P_n(z) > 0$ and $Q_n(z) > 0$.

Proof. Let
\[
\alpha = z + \sqrt{-1}, \quad \beta = z - \sqrt{-1}.
\]
Then we have
\[
\alpha = \sqrt{z^2 + 1} e^{\theta \sqrt{-1}}, \quad \beta = \sqrt{z^2 + 1} e^{-\theta \sqrt{-1}},
\]
where $\theta$ is a real number satisfying
\[
\tan \theta = \frac{1}{z}, \quad 0 \leq \theta < \pi.
\]
By (2.1)–(2.3), we have
\[
P_n(z) = \frac{1}{2} (\alpha^n + \beta^n) = (z^2 + 1)^{n/2} \cos(n \theta),
\]
\[
Q_n(z) = \frac{1}{2 \sqrt{-1}} (\alpha^n - \beta^n) = (z^2 + 1)^{n/2} \sin(n \theta).
\]
Since $z > 2n/\pi$ and
\[
0 < \theta = \arctan \frac{1}{z} < \frac{1}{z},
\]
by (2.4), we get $0 < n \theta < n/z < \pi/2$. It implies that $\cos(n \theta) > 0$ and $\sin(n \theta) > 0$. Thus, by (2.5), the lemma is proved.

Lemma 2.2. For any positive even integer $r$, we have $\lambda_1 P_n(r) + \lambda_2 Q_n(r) \neq (r - 1)^n$, where $\lambda_1, \lambda_2 \in \{\pm 1\}$.

Proof. We now assume that
\[
\lambda_1 P_n(r) + \lambda_2 Q_n(r) = (r - 1)^n, \quad r \in \mathbb{N}, \ 2|r, \ \lambda_1, \ \lambda_2 \in \{\pm 1\}.
\]
By (2.1), we have
\[
P_n(r) = (-1)^{(n-1)/2} \sum_{i=0}^{(n-1)/2} (-1)^i \binom{n}{2i+1} r^{2i+1},
\]
\[ Q_n(r) = (-1)^{(n-1)/2} \sum_{i=0}^{(n-1)/2} (-1)^i \binom{n}{2i} r^{2i}. \] 

(2.8)

Substituting (2.8) into (2.7), we get

\[ (-1)^{(n-1)/2} \lambda_2 \equiv -1 \pmod{r}. \] 

(2.9)

If \((-1)^{(n-1)/2} \lambda_2 = 1\), then from (2.9) we get \(2 \equiv 0 \pmod{r}\) and \(r = 2\). Notice that

\[ P_n(2) \equiv (-1)^{(n-1)/2} 2n \pmod{4}, \quad Q_n(2) \equiv (-1)^{(n-1)/2} (mod 4) \text{ and } (2-1)^n \equiv 1 \pmod{4}. \]

From (2.7) we get

\[ (-1)^{(n-1)/2} 2n \lambda_1 + (-1)^{(n-1)/2} \lambda_2 \equiv (-1)^{(n-1)/2} 2n \lambda_1 + 1 \equiv 1 \pmod{4}, \] 

(2.10)

whence we obtain \(2|n\), a contradiction.

If \((-1)^{(n-1)/2} \lambda_2 = -1\), then from (2.7) we get \((-1)^{(n-1)/2} \lambda_1 = 1\) and

\[ \binom{n}{2} = \sum_{j=3}^{n} \lambda_j \binom{n}{j} r^{j-2}, \quad \lambda_j \in \{0, \pm 1\}, \quad j \geq 3. \] 

(2.11)

This time, if \(r = 2\), then it can be deal with by arguments similar to the ones from the case \((-1)^{(n-1)/2} \lambda_2 = 1\). If \(r > 2\), let \(2^\alpha \parallel (n-1)/2\) and \(2^\beta_j \parallel j(j-1)\) for \(j \geq 3\). Since \(2|r, \beta_3 = 1\) and \(\beta_j \leq (\log j)/\log 2 \leq j-2\) for \(j \geq 4\), by

\[ \binom{n}{j} r^{j-2} = n \binom{n-1}{2} \binom{n-2}{j-2} \frac{2r^{j-2}}{j(j-1)}, \] 

(2.12)

we get

\[ \binom{n}{j} r^{j-2} \equiv 0 \pmod{2^{\alpha+1}}, \quad j \geq 3. \] 

(2.13)

Therefore, since \(2^\alpha \parallel \left(\binom{n}{2}\right)\), we see from (2.13) that (2.11) is impossible. It implies that (2.7) is false. The lemma is proved.

**Lemma 2.3.** If \(z > 5(n-1)/2\), then \(P_n(z) - Q_n(z) > (z-3)^n\).

**Proof.** We now assume that

\[ P_n(z) - Q_n(z) \leq (z-3)^n. \] 

(2.14)

By (2.1) and (2.14), we have

\[ \sum_{i=0}^{(n-1)/2} \left(\binom{n}{2i+1} (3^{2i+1} - (-1)^i) z^{n-2i-1} \right. 

- \left. \binom{n}{2i+2} (3^{2i+2} + (-1)^i) z^{n-2i-2} \right) \leq 0. \] 

(2.15)
However, since $z > 5(n - 1)/2$, we have 
\[
\begin{align*}
\left( \frac{n}{2i+1} \right) ((3^{2i+1} - (-1)^i) z^{n-2i-1} - \left( \frac{n}{2i+2} \right) (3^{2i+2} + (-1)^i) z^{n-2i-2} \\
= \left( \frac{n}{2i+1} \right) ((3^{2i+1} - (-1)^i) z^{n-2i-2} \\
\times (z - \left( \frac{n - 2i - 1}{2i+2} \right) \left( \frac{3^{2i+2} + (-1)^i}{3^{2i+1} - (-1)^i} \right)) \\
\geq \left( \frac{n}{2i+1} \right) ((3^{2i+1} - (-1)^i) z^{n-2i-2} (z - \frac{5}{2}(n - 1)) > 0, \quad j \geq 0. (2.16)
\end{align*}
\]
Therefore, by (2.16), (2.15) is impossible. The lemma is proved. \qed

Lemma 2.4 ([7, Section 15.2]). For any positive odd integer $n$, every solution of the equation
\[
X^2 + Y^2 = Z^n, \quad X, Y, Z \in \mathbb{N}, \quad \gcd(X, Y) = 1, \ 2|X
\] (2.17)
can be expressed as 
\[
Z = r^2 + s^2, \quad r, s \in \mathbb{N}, \quad \gcd(r, s) = 1, \ 2|r, \\
X + Y\sqrt{-1} = \lambda_1 (r + \lambda_2 s \sqrt{-1})^n, \quad \lambda_1, \ \lambda_2 \in \{ \pm 1 \}.
\]

Let $\alpha, \ \beta$ be algebraic integers. If $\alpha + \beta$ and $\alpha\beta$ are nonzero coprime integers and $\alpha/\beta$ is not a root of unity, then $(\alpha, \ \beta)$ is called a Lucas pair. Further, let $A = \alpha + \beta$ and $C = \alpha\beta$. Then we have
\[
\alpha = \frac{1}{2} (A + \lambda \sqrt{B}), \quad \beta = \frac{1}{2} (A - \lambda \sqrt{B}), \quad \lambda \in \{ \pm 1 \},
\]
where $B = A^2 - 4C$. We call $(A, \ B)$ the parameters of the Lucas pair $(\alpha, \ \beta)$. Two Lucas pairs $(\alpha_1, \ \beta_1)$ and $(\alpha_2, \ \beta_2)$ are equivalent if $\alpha_1/\alpha_2 = \beta_1/\beta_2 = \pm 1$. Given a Lucas pair $(\alpha, \ \beta)$, one defines the corresponding sequence of Lucas numbers by
\[
L_k(\alpha, \ \beta) = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \quad k = 0, 1, 2, \ldots. \tag{2.18}
\]
For equivalent Lucas pairs $(\alpha_1, \ \beta_1)$ and $(\alpha_2, \ \beta_2)$, we have $L_k(\alpha_1, \ \beta_1) = \pm L_k(\alpha_2, \ \beta_2)$ for any $k$. A prime $I$ is called a primitive divisor of $L_k(\alpha, \ \beta)$ if $k > 1, I|L_k(\alpha, \ \beta)$ and $I \nmid BL_1(\alpha, \ \beta) \cdots L_{k-1}(\alpha, \ \beta)$. A Lucas pair $(\alpha, \ \beta)$ such that $L_k(\alpha, \ \beta)$ has no primitive divisor will be called a $k$-defective Lucas pair. Further, a positive integer $k$ is called totally nondefective if no Lucas pair is $k$-defective.

Lemma 2.5 ([9]). Let $k$ satisfy $4 < k \leq 30$ and $k \neq 6$. Then, up to equivalence, all parameters of $k$-defective Lucas pairs are given as follows:

(i) $k = 5, (A, \ B) = (1, \ 5), (1, \ -7), (2, \ -40), (1, \ -11), (1, \ -15), (12, \ -76), (12, \ -1364)$.
(ii) $k = 7, (A, \ B) = (1, \ -7), (1, \ -19)$. 

(iii) \( k = 8, (A, B) = (2, -24), (1, -7) \).
(iv) \( k = 10, (A, B) = (2, -8), (5, -3), (5, -47) \).
(v) \( k = 12, (A, B) = (1, 5), (1, -7), (1, -11), (2, -56), (1, -15), (1, -19) \).
(vi) \( k \in \{13, 18, 30\}, (A, B) = (1, -7) \).

Lemma 2.6 ([1]). If \( k > 30 \), then \( k \) is totally nondefective.

3. Proof of theorem

Lemma 3.1. Let \((x, y)\) be a solution of (1.2) with \( 2 \not\mid y \). If \( n > 3 \) and \( p \equiv 3 \mod 4 \), then we have
\[
\begin{align*}
x &= |P_n(r)|, \\
q &= |Q_n(r)|, \\
r &\in \mathbb{N}, 2|r 
\end{align*}
\] (3.1)
and
\[
\begin{align*}
x + \lambda q &= c^n, \\
x - \lambda q &= pd^n, \\
y &= cd(r^2 + 1), \\
\lambda &\in \{\pm 1\}, \\
c, d &\in \mathbb{N}, \gcd(c, d) = 1, 2 \not\mid cd. 
\end{align*}
\] (3.2)

Proof. Since \( 2 \not\mid qy \), we have \( 2 \mid x \). Since \( \gcd(x, y) = 1 \), we get \( q \not\mid xy \) and \( \gcd(x^2 - q^2, x^2 + q^2) = 1 \). Further, since \( p \equiv 3 \mod 4 \), we have \( p \not\mid x^2 + q^2 \). Therefore, by (1.2), we get
\[
\begin{align*}
x^2 - q^2 &= pa^n, \\
x^2 + q^2 &= b^n, \\
y &= ab, \\
a, b &\in \mathbb{N}, \\
\gcd(a, b) = 1, 2 \not\mid ab. 
\end{align*}
\] (3.3)

By the first equality of (3.3), we have
\[
\begin{align*}
x + \lambda q &= c^n, \\
x - \lambda q &= pd^n, \\
a &= cd, \\
c, d &\in \mathbb{N}, \\
\gcd(c, d) = 1, 2 \not\mid cd. 
\end{align*}
\] (3.4)

Applying Lemma 2.4 to the second equality of (3.3), we get
\[
\begin{align*}
b &= r^2 + s^2, \\
r, s &\in \mathbb{N}, \\
\gcd(r, s) = 1, 2|r 
\end{align*}
\] (3.5)
and
\[
\begin{align*}
x + q\sqrt{-1} &= \lambda_1 r + \lambda_2 s\sqrt{-1} n, \\
\lambda_1, \lambda_2 &\in \{\pm 1\}. 
\end{align*}
\] (3.6)

From (3.6), we have
\[
x = \lambda_1 r \sum_{i=0}^{(n-1)/2} \binom{n}{2i} r^{n-2i-1} (-s^2)^i 
\] (3.7)
and
\[
q = \lambda_1 \lambda_2 s \sum_{i=0}^{(n-1)/2} \binom{n}{2i+1} r^{n-2i-1} (-s^2)^i. 
\] (3.8)
Further, since $q$ is an odd prime, we get from (3.8) that either

$$s = q, \quad 1 = \lambda_1 \lambda_2 \sum_{i=0}^{(n-1)/2} \left( \frac{n}{2i+1} \right) r^{n-2i-1} (-q^2)^i$$

(3.9)

or

$$s = 1, \quad q = \lambda_1 \lambda_2 \sum_{i=0}^{(n-1)/2} (-1)^i \left( \frac{n}{2i+1} \right) r^{n-2i-1}.$$  

(3.10)

We now remove the possibility of (3.9). Let

$$\alpha = r + q \sqrt{-1}, \quad \beta = r - q \sqrt{-1}. \quad (3.11)$$

Then we have $\alpha + \beta = 2r$, $\alpha \beta = r^2 + q^2$ and $\alpha / \beta$ satisfies $(r^2 + q^2)(\alpha / \beta)^2 - 2(r^2 - q^2)(\alpha / \beta) + (r^2 + q^2) = 0$. It implies that $\alpha + \beta$ are coprime positive integers, and $\alpha / \beta$ is not a root of unity. Therefore, $(\alpha, \beta)$ is a Lucas pair with parameters $(2r, -4q^2)$. Let $L_k(\alpha, \beta)$ $(k = 0, 1, 2, \ldots)$ denote the corresponding Lucas numbers. If (3.9) holds, then from (2.18) and (3.11) we get

$$L_n(\alpha, \beta) = \pm 1.$$  

(3.12)

We see from (3.12) that the Lucas number $L_n(\alpha, \beta)$ has no primitive divisor. But, since $n$ is an odd prime with $n > 3$, by Lemmas 2.5 and 2.6, it is impossible. Therefore, (3.9) is impossible.

Since $s = 1$ by (3.10), comparing (2.1), (3.7) and (3.8), we obtain (3.1). Moreover, by (3.3)–(3.5), we get (3.2). Thus, the theorem is proved.

**Proof of Theorem.** Let $(x, y)$ be a solution of (1.2) with $2 \nmid y$. By Lemma 3.1, $x, y$ and $q$ satisfy (3.1) and (3.2). We see from (2.1) and (3.1) that

$$x - q < x + q \leq |P_n(r)| + |Q_n(r)| < (r + 1)^n.$$  

(3.13)

Since $2 \nmid c$, by (3.2) and (3.13), we have $c \leq r - 1$. Further, by Lemma 2.2, we have $c^n = x + \lambda q = |P_n(r)| + \lambda |Q_n(r)| \neq (r - 1)^n$. It implies that $c \neq r - 1$ and

$$c \leq r - 3.$$  

(3.14)

We now remove the existence of the solution $(x, y)$ in the following three cases.

Case I: $r > 5(n - 1)/2$.

By Lemma 2.1, we get from (3.1) that

$$x = P_n(r), \quad q = Q_n(r).$$  

(3.15)

Further, by Lemma 2.3, we obtain from (3.2), (3.14) and (3.15) that

$$(r - 3)^n \geq c^n = x + \lambda q \geq x - q > (r - 3)^n,$$  

(3.16)

a contradiction.
Case II: \(2n/\pi < r \leq 5(n - 1)/2\).

By Lemma 2.1, \(x\) and \(q\) satisfy (3.15) too. Since \(n\) is an odd prime, we have
\[
\binom{n}{0} = \binom{n}{n} = 1, \quad n \mid \binom{n}{j}, \quad j = 1, \ldots, n - 1.
\] (3.17)

Hence, by (2.1) and (3.17), we have
\[
P_n(r) \equiv r^n \equiv r \pmod{n}, \quad Q_n(r) \equiv (-1)^{(n-1)/2} \pmod{n}.
\] (3.18)

Substituting (3.18) into (3.15), we get from (3.2) that
\[
c \equiv c^n \equiv x + \lambda q \equiv r + (-1)^{(n-1)/2} \lambda \pmod{n}, \quad \lambda \in \{\pm 1\}.
\] (3.19)

Further, since \(2 \mid r\) and \(2 \nmid cn\), by (3.19), we have
\[
c \equiv r + (-1)^{(n-1)/2} \lambda \pmod{2n}.
\] (3.20)

Since \(2n/\pi < r \leq 5(n - 1)/2\), we see from (3.14) and (3.20) that
\[
c = r + (-1)^{(n-1)/2} \lambda - 2n \leq r + 1 - 2n.
\] (3.21)

Hence, by (3.21), we have
\[
r \geq 2n, \quad c < \frac{n}{2} \leq \frac{r}{4}.
\] (3.22)

By (2.4), (2.5), (3.15) and (3.22), we get
\[
x + \lambda q \geq x - q = P_n(r) - Q_n(r) = (r^2 + 1)^{n/2} \cos(n\theta) - \sin(n\theta)) \geq (r^2 + 1)^{n/2} \sqrt{2} \cos\left(n\theta + \frac{\pi}{4}\right),
\] (3.23)

where \(\theta\) is a real number satisfying
\[
0 < n\theta = n \arctan \frac{1}{r} < \frac{n}{r} \leq \frac{1}{2}.
\] (3.24)

Therefore, by (3.2) and (3.22)–(3.24), we obtain
\[
\left(\frac{r}{4}\right)^n > c^n = x + \lambda q > (r^2 + 1)^{n/2} \sqrt{2} \cos\left(\frac{1}{2} + \frac{\pi}{4}\right) > 0.3897(r^2 + 1)^{n/2} > 0.3897r^n,
\] (3.25)

whence we get \(1 > 0.3897 \times 4^n > 1\), a contradiction.

Case III: \(r \leq 2n/\pi\).

By (3.1), (3.2) and (3.18), we get
\[
c \equiv c^n \equiv x + \lambda q \equiv |P_n(r)| + \lambda |Q_n(r)| \equiv \lambda_1 r + \lambda_2 \pmod{2n}, \quad \lambda, \lambda_1, \lambda_2 \in \{\pm 1\}.
\] (3.26)

But, since \(0 < r < 2n/\pi < n\) and \(0 < c \leq r - 3\) by (3.14), (3.26) is impossible.

To sum up, we deduce that (1.2) has no solution \((x, y)\) with \(2 \nmid y\). The theorem is proved. \(\square\)
Acknowledgments

The author would like to thank the referee for his very helpful and detailed comments, which have significantly improved the presentation of this paper. This work is supported by the Foundation of Tibet University For Nationalities, PR China.

References