Bull. Math. Soc. Sci. Math. Roumanie
Tome 60 (108) No. 1, 2017, 51–57

A note on the Diophantine equation $px^2 + q^{2n} = y^p$

by
Wang Xiaoying and Zhang Han

Abstract

Let $p,\ q$ be odd primes such that $p \equiv 1(\bmod\ 4)$ and $p \neq q$. In this paper, we prove that if $q < 4p - 1$ or $q < 149$, then the equation $px^2 + q^{2n} = y^p$ has no positive integer solutions (x, y, n) with $\gcd(x, y) = 1$.

Key Words: exponential diophantine equation; class number of binary quadratic forms; primitive divisor of Lehmer numbers.
2010 Mathematics Subject Classification: 11D61.

1 Introduction

Let $\mathbb{Z}, \mathbb{N}$ be the sets of all integers and positive integers respectively. Let p be an odd prime with $p \not\equiv 7(\bmod\ 8)$ and let q be a prime with $q \neq p$. The solutions (x, y, n) of the equation

$$px^2 + q^{2n} = y^p\,, \quad x, y, n \in \mathbb{N},\ \gcd(x, y) = 1 \tag{1.1}$$

and its varieties have been investigated in many papers (see [1], [2], [5], [7], [8], [10], [11], [12], [14] and [15]).

For instance, by the results of S.Rabinowicz [11], M.-H.Le [8] and F.S. Abu Muriefah [1], if $q \in \{2, 3\}$, then (1.1) has no solutions (x, y, n). Let $p,\ q$ be primes and $p > 3$. Let further x,y and n be positive integers such that $(x, y) = 1$. In [2], F.S. Abu Muriefah was solved (1.1) completely. Recently, A. Laradji, M. Mignotte and N. Tzanakis [7] proved that if $p \equiv 3(\bmod\ 8)$, then (1.1) has no solutions (x, y, n). In [14], W. Yongxing and W. Tingting proved that the Diophantine equation $2^m + nx^2 = y^n$ has no positive integer solution (x, y, m) with $\gcd(x, y) = 1$. In [10], it was proved that the Diophantine equation $2^m + nx^2 = y^n$ in positive integers x, y, m, n has the only solution $(x, y, m, n) = (21, 11, 3, 3)$ with $n > 1$ and $\gcd(nx, y) = 1$ by F. Luca and G. Soydan. In [12], G. Soydan, and I.N. Cangul, noted corrections to the paper of W. Yongxing and W. Tingting [14].

For the remained cases, namely $p \equiv 1(\bmod\ 4)$, the solving of (1.1) is a very difficult problem, even when $p = 5$ it is still open. By [7], if $p = 5$ and either $q \not\equiv 1(\bmod\ 600)$ or $q < 3 \times 10^9$, then (1.1) has no solutions (x, y, n).

In this paper, using certain properties of exponential diophantine equations and the existence results of primitive divisors of Lehmer numbers, we shall show that (1.1) has no solutions for small q. We prove the following result:

Theorem. *Let $p,\ q$ be odd primes such that $p \equiv 1(\bmod 4)$ and $p \neq q$, if $q < 4p - 1$ or $q < 149$, then (1.1) has no solutions (x, y, n).*

2 Preliminaries

For any positive integer d, let $h(-4d)$ denote the class number of positive binary quadratic forms of discriminant $-4d$.

Lemma 1. *([15, Lemma 3]). If $d > 1$, then $d > h(-4d)$.*

Lemma 2. *If $p \equiv 1 (\bmod\ 4)$ and q is an odd prime with $q \neq p$, then*

$$h(-4pq^2) = \left(q - (-1)^{(q-1)/2}\left(\frac{q}{p}\right)\right) h(-4p), \tag{2.1}$$

where $\left(\frac{q}{p}\right)$ is the Kronecker symbol.

Proof: Since $p \equiv 1(\bmod\ 4)$, $-4p \equiv 12 (\bmod\ 16)$ and $-4p$ is a fundamental discriminant. Hence, by Theorems 12.10.1 and 12.11.2 of [6], we have

$$h(-4p) = \frac{2\sqrt{p}}{\pi} K(-4p) \tag{2.2}$$

and

$$h(-4pq^2) = \frac{2q\sqrt{p}}{\pi} K(-4pq^2) = \frac{2q\sqrt{p}}{\pi}\left(1 - \left(\frac{-4p}{q}\right)\frac{1}{q}\right) K(-4p),$$

where

$$K(-4p) = \sum_{m=1}^{\infty}\left(\frac{-4p}{m}\right)\frac{1}{m}.$$

The combination of (2.2) and (2.3) yields

$$h(-4pq^2) = \left(q - \left(\frac{-4p}{q}\right)\right) h(-4p). \tag{2.4}$$

Further, since $p \equiv 1(\bmod\ 4)$ and q is an odd prime with $q \neq p$,

$$\left(\frac{-4p}{q}\right) = (-1)^{(q-1)/2}\left(\frac{4p}{q}\right) = (-1)^{(q-1)/2}\left(\frac{p}{q}\right) = (-1)^{(q-1)/2}\left(\frac{q}{p}\right). \tag{2.5}$$

Substitute (2.5) into (2.4), we get (2.1) immediately. So, the proof is completed. □

Lemma 3. *([9,Theorems 1 and 3]). Let d_1, d_2, k be positive integers such that $\min\{d_1, d_2, k\} > 1$ and $\gcd(d_1, d_2)=\gcd(k, 2d_1d_2) = 1$. If the equation*

$$d_1X^2 + d_2Y^2 = k^Z, X, Y, Z \in \mathbb{Z},\ \gcd(X, Y) = 1, Z > 0 \tag{2.6}$$

has solutions (X, Y, Z), then every solution (X, Y, Z) of (2.6) can be expressed as

$$Z = Z_1 t,\ t \in \mathbb{N},\ 2 \nmid t,$$

$$X\sqrt{d_1} + Y\sqrt{-d_2} = \lambda_1(X_1\sqrt{d_1} + \lambda_2 Y_1\sqrt{-d_2})^t,\ \lambda_1, \lambda_2 \in \{\pm 1\},$$

where X_1, Y_1, Z_1 are positive integers satisfying

$$d_1{X_1}^2 + d_2{Y_1}^2 = k^{Z_1}, \gcd(X_1, Y_1) = 1, 2Z_1 \mid h(-4d_1d_2).$$

Lemma 4. *([3, Theorem 1.1]). If $p \in \{13, 17\}$, then the equation*

$$X^n + Y^n = pZ^2, X, Y, Z \in \mathbb{Z}, XYZ \neq 0, X > Y, \gcd(X, Y) = 1, n \in \mathbb{N}, n \geq 4. \tag{2.7}$$

has no solution (X, Y, Z, n).

Lemma 5. *([7, Proposition 2.1]). If (x, y, n) is a solution of (1.1), then*

$$q^n = \pm \sum_{i=0}^{(p-1)/2} \binom{p}{2i} \left(-pa^2\right)^i, \text{with } a \in \mathbb{N}, 2 \mid a. \tag{2.8}$$

Let α, β be algebraic integers. If $(\alpha+\beta)^2$ and $\alpha\beta$ are nonzero coprime integers and α/β is not a root of unity, then (α, β) is called a Lehmer pair. Further, let $a = (\alpha+\beta)^2$ and $c = \alpha\beta$. Then we have

$$\alpha = \frac{1}{2}(\sqrt{a} + \lambda\sqrt{b}), \beta = \frac{1}{2}(\sqrt{a} - \lambda\sqrt{b}), \lambda \in \{\pm 1\},$$

where $b = a - 4c$. Such (a, b) is called the parameters of Lehmer pair (α, β). Two Lehmer pairs (α_1, β_1) and (α_2, β_2) are called equivalent if $\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \left\{\pm 1, \pm\sqrt{-1}\right\}$. Obviously, if (α_1, β_1) and (α_2, β_2) are equivalent Lehmer pairs with parameters (a_1, b_1) and (a_2, b_2) respectively, then $(a_2, b_2) = (\delta a_1, \delta a_2)$, where $\delta \in \{\pm 1\}$. For a fixed Lehmer pair (α, β), one defines the corresponding sequence of Lehmer numbers by

$$L_r(\alpha, \beta) = \begin{cases} \frac{\alpha^r - \beta^r}{\alpha - \beta}, & \text{if } 2 \nmid r, \\ \frac{\alpha^r - \beta^r}{\alpha^2 - \beta^2}, & \text{if } 2 \mid r, \end{cases}, \quad r \in \mathbb{N}. \tag{2.9}$$

Then, Lehmer numbers $L_r(\alpha, \beta)$ $(r = 1, 2, \cdots)$ are nonzero integers. Further, for equivalent Lehmer pairs (α_1, β_1) and (α_2, β_2), we have $L_r(\alpha_1, \beta_1) = \pm L_r(\alpha_2, \beta_2)$ for any r. A prime l is called a primitive divisor of the Lehmer number $L_r(\alpha, \beta)$ $(r > 1)$, if $l \mid L_r(\alpha, \beta)$ and $l \nmid abL_1(\alpha, \beta) \cdots L_{r-1}(\alpha, \beta)$, where (a, b) is the parameter of Lehmer pair (α, β). A Lehmer pair (α, β) such that $L_r(\alpha, \beta)$ has no primitive divisor will be called r-defective Lehmer pair.

Lemma 6. *([13]). Let r be such that $6 < r \leq 30$ and $r \neq 8, 10, 12$. Then, up to equivalence, all parameters (a, b) $(a > 0)$ of r-defective Lehmer pairs are given as follows:*
(i) $r = 7, (a, b) = (1, -7), (1, -19), (3, -5), (5, -7), (13, -3), (14, -22)$.
(ii) $r = 9, (a, b) = (5, -3), (7, -1), (7, -5)$.
(iii) $r = 13, (a, b) = (1, -7)$.
(iv) $r = 14, (a, b) = (3, -13), (5, -3), (7, -1), (7, -5), (19, -1), (22, -14)$.
(v) $r = 15, (a, b) = (7, -1), (10, -2)$.
(vi) $r = 18, (a, b) = (1, -7), (3, -5), (5, -7)$.
(vii) $r = 24, (a, b) = (3, -5), (5, -3)$.
(viii) $r = 26, (a, b) = (7, -1)$.
(ix) $r = 30, (a, b) = (1, -7), (2, -10)$.

Lemma 7. *([4, Theorem 1.4]). If $r > 30$, then no Lehmer pair is r-defective.*

3 Proof of Theorem

Lemma 8. *If (1.1) has solutions* (x, y, n)*, then* $p \equiv 1 (\mathrm{mod}\ 4)$ *and*

$$q - (-1)^{(q-1)/2} \equiv 0 (\mathrm{mod}\ 4p)\,. \tag{3.1}$$

In particular, if $p \nmid n$*, then*

$$q - (-1)^{(q-1)/2} \equiv 0 (\mathrm{mod}\ 4p^2). \tag{3.2}$$

Proof: We now assume that (x, y, n) is a solution of (1.1). By the results of [7], we have $p \equiv 1 (\mathrm{mod}\ 4)$ and the lemma holds for $p = 5$. Then, by (1.1), the equation

$$pX^2 + q^2 Y^2 = y^Z, X, Y, Z \in \mathbb{Z},\ \gcd(X, Y) = 1,\ Z > 0 \tag{3.3}$$

has a solution

$$(X, Y, Z) = (x, q^{n-1}, p). \tag{3.4}$$

Since $p \equiv 1 (\mathrm{mod}\ 4)$, y is odd. Applying Lemma 3 to (3.3) and (3.4), we have

$$p = Z_1 t,\ t \in \mathbb{N},\ 2 \nmid t, \tag{3.5}$$

$$x\sqrt{p} + q^{n-1}\sqrt{-q^2} = \lambda_1 (X_1\sqrt{p} + \lambda_2 Y_1 \sqrt{-q^2})^t,\ \lambda_1, \lambda_2 \in \{\pm 1\}\,, \tag{3.6}$$

where X_1, Y_1, Z_1 are positive integers satisfying

$$pX_1{}^2 + q^2 Y_1{}^2 = y^{Z_1}, \gcd(X_1, Y_1) = 1 \tag{3.7}$$

and

$$2Z_1 \mid h(-4pq^2). \tag{3.8}$$

If $Z_1 = 1$, then from (3.5), (3.6) and (3.7) we get

$$x\sqrt{p} + q^{n-1}\sqrt{-q^2} = \lambda_1 (X_1\sqrt{p} + \lambda_2 Y_1 \sqrt{-q^2})^p,\ \lambda_1, \lambda_2 \in \{\pm 1\}\,, \tag{3.9}$$

and

$$pX_1{}^2 + q^2 Y_1{}^2 = y, X_1, Y_1 \in \mathbb{N},\ \gcd(X_1, Y_1) = 1. \tag{3.10}$$

By (3.9), we have

$$q^{n-1} = Y_1 \sum_{i=0}^{(p-1)/2} \binom{p}{2i+1} (pX_1{}^2)^{(p-1)/2-i} (-q^2 Y_1{}^2)^i. \tag{3.11}$$

Since $p \neq q$ and $\gcd(x, y) = 1$, we see from (1.1) and (3.10) that $q \nmid y$ and $q \nmid pX_1{}^2$. It implies that

$$q \nmid \sum_{i=0}^{(p-1)/2} \binom{p}{2i+1} (pX_1{}^2)^{(p-1)/2-i} (-q^2 Y_1{}^2)^i. \tag{3.12}$$

Therefore, by (3.11) and (3.12), we get

$$Y_1 = q^{n-1} \tag{3.13}$$

and

$$\sum_{i=0}^{(p-1)/2} \binom{p}{2i+1} (p{X_1}^2)^{(p-1)/2-i}(-q^{2n})^i = \pm 1. \tag{3.14}$$

Let

$$\alpha = \sqrt{p{X_1}^2} + \sqrt{-q^{2n}}, \beta = \sqrt{p{X_1}^2} - \sqrt{-q^{2n}}. \tag{3.15}$$

Then, (α, β) is a Lehmer pair with parameters $(4p{X_1}^2, -4q^{2n})$. Further let $L_r(\alpha, \beta)$ $(r = 1, 2, \cdots)$ denote the Lehmer numbers defined by (2.9). We get from (3.14) and (3.15) that

$$L_p(\alpha, \beta) = \pm 1. \tag{3.16}$$

It implies that the Lehmer number $L_p(\alpha, \beta)$ has no primitive divisor. But, since $p > 5$ and $p \equiv 1 (\mathrm{mod}\ 4)$, by Lemmas 6 and 7, (3.16) is false. So we have $Z_1 \neq 1$.

Since $Z_1 \neq 1$ and p is an odd prime, by (3.5), we get $Z_1 = p$. Substitute it into (3.8), we have

$$2p \mid h(-4pq^2). \tag{3.17}$$

Further, applying Lemma 2.2 to (3.17), we get

$$2p \mid \left(q - (-1)^{(q-1)/2} \left(\frac{q}{p} \right) \right) h(-4p). \tag{3.18}$$

By Lemma 1, we have $p > h(-4p)$ and $p \nmid h(-4p)$. Therefore, by (3.18), we obtain

$$p \mid q - (-1)^{(q-1)/2} \left(\frac{q}{p} \right). \tag{3.19}$$

Notice that $p \equiv 1 (\mathrm{mod}\ 4), (q/p) = \pm 1$ and $q \equiv \pm 1 (\mathrm{mod}\ p)$ by (3.19). We have $(q/p) = (\pm 1/p) = 1$. Thus, by (3.19), we get

$$p \mid q - (-1)^{(q-1)/2}. \tag{3.20}$$

Since $4 \mid q - (-1)^{(q-1)/2}$, we see from (3.20) that if (1.1) has solutions, then p and q satisfy (3.1).

Finally, by Lemma 5, we get from (3.20) that

$$q^n - (-1)^{n(q-1)/2} \equiv 0 (\mathrm{mod}\ 4p^2). \tag{3.21}$$

Therefore, if $p \nmid n$, then from (3.21) we get (3.2). Thus, the lemma is proved. □

Lemma 9. *If $q - (-1)^{(q-1)/2}$ has no odd prime divisor p satisfying the following conditions, then (1.1) has no solutions (x, y, n):*
(i) $p = 5$ *and* $p^3 \mid q - (-1)^{(q-1)/2}$.
(ii) $p \in \{13, 17\}$ *and* $p^2 \mid q - (-1)^{(q-1)/2}$.
(iii) $p \equiv 1 (\mathrm{mod}\ 4)$ *and* $p > 17$.

Proof: By the results of [7] and Lemma 8, if (1.1) has solutions (x, y, n), then $q-(-1)^{(q-1)/2}$ has an odd prime divisor p with $p \equiv 1(\bmod\ 4)$. Moreover, if $p = 5$, then $p^3 \mid q-(-1)^{(q-1)/2}$. Therefore, the conditions (i) and (iii) are proved.

Obviously, if (1.1) has solutions (x, y, n) with $p \mid n$, then (2.7) has the solutions $(X, Y, Z, n) = (y^{n/p}, -q^{2n/p}, x, p)$. Therefore, by Lemmas 2.5 and 3.1, if $p \in \{13, 17\}$, then $p^2 \mid q - (-1)^{(q-1)/2}$ and the condition (ii) holds. Thus, the lemma is proved. □

Proof of Theorem.

By Lemma 8, if (1.1) has solutions (x, y, n), then p and q satisfy (3.1). It implies that $q + 1 \geq q - (-1)^{(q-1)/2} \geq 4p$ and $q \geq 4p - 1$. Therefore, if $q < 4p - 1$, then (1.1) has no solutions.

On the other hand, using an easy computation, if $q < 149$, then q does not satisfy the conditions of Lemma 9.

Therefore, if $q < 149$, then (1.1) has no solutions (x, y, n). Thus, the theorem is proved. □

Acknowledgement. This paper is supported by N. S. F. (11371291) and P. N. S. F. (2013JM1017) of P. R. China and G.I.C.F.(YZZ14004) of NWU. P.R. China. The authors would like to thank the referee for his very helpful and detailed comments, which have significantly improved the presentation of this paper.

References

[1] Abu Muriefah, F.S., On the diophantine equation $px^2 + 3^n = y^p$, *Tamkang J. Math.*, **31(1)** (2000), 79-84.

[2] Abu Mureifah, F.S., On the diophantine equation $px^2 + q^{2m} = y^p$, *J. Number Theory*, **128(6)** (2008), 1670-1675.

[3] Bennett, M. A. and Skinner, C. M., Ternary diophantine equations via Galois representations and modular forms, *Canad. J. Math.*, **56(1)** (2004), 23-54.

[4] Bilu, Y., Hanrot, G. and Voutier, P. M. (with an appendix by Mignotte, M.), Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.*, **539** (2001), 75-122.

[5] Goedhat, E. G. and Grundman, H. G., On the diophantine equation $NX^2 + 2^L \cdot 3^M = Y^N$, *J. Number Theory*, **141(2)** (2014), 214-224.

[6] Hua L.-G., *Introdution to number theory*, Berlin: Springer Verlag, 1982.

[7] Laradji, A.,Mignotte, M. and Tzanakis, N., On $px^2 + q^{2n} = y^p$ and related diophantine equations, *J. Number Theory*, **131(8)** (2011), 1575-1596.

[8] Le M.-H., On the diophantine equation $2^n + px^2 = y^p$, *Proc. Amer. Math. Soc.*, **123(2)** (1995), 321-326.

[9] Le M.-H., Some exponential diophantine equations I: The equation $D_1x^2 - D_2y^2 = \lambda k^Z$, *J. Number Theory*, **55(2)** (1995), 209-221.

[10] Luca, F. and Soydan, G., On the diphantine equation $2^m + nx^2 = y^n$, *J. Number Theory*, **132(11)** (2012), 2604-2609.

[11] Rabinowitz, S., The solution of $3y^2 \pm 2^n = x^3$, *Proc. Amer. Math. Soc.*, **69(3)** (1978), 213-218.

[12] Soydan, G. and Cangul, I. N., Note on "On the diophantine equation $nx^2+2^{2m} = y^n$", *J. Number Theory*, **140(2)** (2014), 425-426.

[13] Voutier, P. M., Primitive divisors of Lucas and Lehmer sequences, *Math. Comp.*, **64** (1995), 869-888.

[14] Wang Y.-X. and Wang T.-T., On the diophantine equation $nx^2 + 2^{2m} = y^n$, *J. Number Theory*, **131(8)** (2011), 1486-1491.

[15] Wu H.-M., The diophantine equation $nx^2 + 2^m = y^n$, *Adv. Math. China*, **40(3)** (2011), 365-369.

Received: 06.03.2015
Revised: 12.04.2016
Accepted: 13.04.2016

School of Mathematics,
Northwest University
E-mail: xdwxy@163.com
micohanzhang@hotmail.com