Bull. Aust. Math. Soc. **86** (2012), 303–314
doi:10.1017/S000497271200010X

ON THE EXPONENTIAL DIOPHANTINE EQUATION $x^2 + p^{2m} = 2y^n$

HUILIN ZHU✉, MAOHUA LE and ALAIN TOGBÉ

(Received 22 October 2011)

Abstract

Let p be an odd prime. In this paper, we consider the equation

$$x^2 + p^{2m} = 2y^n, \quad \gcd(x, y) = 1, n > 2,$$

and we describe all its solutions. Moreover, we prove that this equation has no solution (x, y, m, n) when $n > 3$ is an odd prime and y is not the sum of two consecutive squares. This extends the work of Tengely [On the diophantine equation $x^2 + q^{2m} = 2y^p$, *Acta Arith.* **127**(1) (2007), 71–86].

2010 *Mathematics subject classification*: primary 11D61.

Keywords and phrases: exponential Diophantine equation, Lehmer number, primitive divisor.

1. Introduction

Let $\mathbb{Z}$, $\mathbb{N}$ be the sets of all integers and positive integers, respectively. Let p be an odd prime. The equation

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

is an important type of exponential Lebesgue–Ramanujan–Nagell equation. The literature is very rich and there are many papers discussing the solutions (x, y, m, n) of (1.1) for special cases. For examples one can refer to [1, 10, 13, 14, 17, 18]. Ljunggren [10] considered the more general equation

$$Cx^2 + D = 2y^n, \quad x, y, n \in \mathbb{N},$$

and described the solutions when n satisfies certain conditions.

The first author was partly supported by the Fundamental Research Funds for the Central Universities (No. 2011121039). The second author was supported by the National Science Foundation of China (No. 10971184). The third author was supported by Purdue University North Central.

In this paper, we describe all solutions of (1.1). We start with some notation. Let $r, s, t, a, b \in \mathbb{N}$. Write

$$u(t) = \sum_{i=0}^{(t-1)/2} \binom{t}{2i} 2^i, \quad v(t) = \sum_{i=0}^{(t-1)/2} \binom{t}{2i+1} 2^i, \quad 2 \nmid t; \tag{1.2}$$

$$U(t) = \frac{1}{2^{(t-1)/2}} \sum_{i=0}^{(t-1)/2} \binom{t}{2i} 3^i, \quad V(t) = \frac{1}{2^{(t-1)/2}} \sum_{i=0}^{(t-1)/2} \binom{t}{2i+1} 3^i, \quad 2 \nmid t; \tag{1.3}$$

$$\begin{aligned} A(2^r, a, b) &= \sum_{i=0}^{2^{r-1}} \binom{2^r}{2i} a^{2^r-2i}(-b^2)^i, \\ B(2^r, a, b) &= ab \sum_{i=0}^{2^{r-1}} \binom{2^r}{2i+1} a^{2^r-2i-2}(-b^2)^i, \end{aligned} \tag{1.4}$$

with $r \geq 2$, $\gcd(a, b) = 1$, $2 \mid ab$;

$$\begin{aligned} C(t, a) &= \frac{a}{2^{(t-1)/2}} \sum_{i=0}^{(t-1)/2} (-1)^i \binom{t}{2i} a^{t-2i-1}, \\ D(t, a) &= \frac{1}{2^{(t-1)/2}} \sum_{i=0}^{(t-1)/2} (-1)^i \binom{t}{2i+1} a^{t-2i-1}, \end{aligned}$$

with $2 \nmid at$.

The aim of this paper is to prove the following result.

Theorem 1.1. *All solutions of (1.1) are included in the following four cases.*

(i) *If $p=3$, then (1.1) has only the solutions* $(x, y, m, n) = (13, 5, 2, 3)$, $(545, 53, 3, 3)$, *and* $(79, 5, 1, 5)$.

(ii) *If p satisfies*

$$p^s = |A(2^r, a, b) \pm B(2^r, a, b)|, \tag{1.5}$$

then (1.1) has only the solutions

$$(x, y, m, n) = (|A(2^r, a, b) \pm B(2^r, a, b)|, a^2 + b^2, s, 2^r). \tag{1.6}$$

(iii) *If p satisfies*

$$p^s = U(t), \tag{1.7}$$

then (1.1) has only the solutions

$$(x, y, m, n) = (4V^3(t) - 3V(t), 2V^2(t) - 1, s, 3). \tag{1.8}$$

(iv) *If p satisfies*

$$p^s = |D(q, a)|, \tag{1.9}$$

where q is an odd prime, then (1.1) has only the solutions

$$(x, y, m, n) = \begin{cases} (|C(q, 239)|, 13, s, 4q) & \text{when } a = 239, \\ (|C(q, u(t))|, v(t), s, 2q) & \text{when } a = u(t), \\ \left(|C(q, a)|, \dfrac{a^2+1}{2}, s, q\right) & \text{when } a > 1. \end{cases} \tag{1.10}$$

Recently, Tengely [18] used the Gel'fond–Baker method to prove that there exist only finitely many odd primes p such that (1.1) has the solution (x, y, m, n) with $\gcd(x, y) = 1$, $x, y \in \mathbb{N}$, satisfying the condition

$$n > 3 \text{ is an odd prime, } y \text{ is not a sum of two consecutive squares.} \tag{1.11}$$

Using Theorem 1.1, we know that if (1.1) has a solution (x, y, m, n) such that $n > 3$ is an odd prime, then this solution is either in case (i) with the solution

$$p = 3, \quad (x, y, m, n) = (79, 5, 1, 5), \tag{1.12}$$

or in case (iv) with the solution

$$p^s = |D(q, a)|, \quad (x, y, m, n) = \left(|C(q, a)|, \frac{a^2+1}{2}, s, q\right), \tag{1.13}$$

where $q > 3$ is an odd prime. For (1.12), $y = 5 = 2^2 + 1^2$ can be denoted as the sum of two consecutive squares. For (1.13),

$$y = \frac{a^2+1}{2} = \left(\frac{a+1}{2}\right)^2 + \left(\frac{a-1}{2}\right)^2.$$

Therefore, we immediately deduce the following result.

Corollary 1.2. *For any odd prime p, (1.1) has no solution (x, y, m, n) satisfying condition (1.11).*

We organise this paper as follows. In Section 2, we will recall and prove some useful properties related to Pell equations and other exponential equations that we will use to prove Theorem 1.1. In the last section, we combine an elementary method and the deep result of Bilu *et al.* [3] to prove Theorem 1.1.

2. Lemmas

Let D be a positive integer which is not a square. By the results in [12] on Pell equations, we immediately obtain the following two lemmas.

Lemma 2.1. *If the equation*

$$u^2 - Dv^2 = -1, \quad u, v \in \mathbb{N}, \tag{2.1}$$

has a solution (u, v)*, then there exists a unique solution* (u_1, v_1) *of* (2.1) *such that* $u_1 + v_1\sqrt{D} \le u + v\sqrt{D}$*. We call* (u_1, v_1) *the least solution of* (2.1)*. Any solution of* (2.1) *has the form*

$$u + v\sqrt{D} = (u_1 + v_1\sqrt{D})^t, \quad t \in \mathbb{N}, 2 \nmid t.$$

Lemma 2.2. *If the equation*

$$U^2 - DV^2 = -2, \quad U, V \in \mathbb{N}, \tag{2.2}$$

has a solution (U, V)*, then there exists a unique solution* (U_1, V_1) *of* (2.2) *such that* $U_1 + V_1\sqrt{D} \le U + V\sqrt{D}$*. We call* (U_1, V_1) *the least solution of* (2.2)*. Any solution of* (2.2) *has the form*

$$\frac{U + V\sqrt{D}}{\sqrt{2}} = \left(\frac{U_1 + V_1\sqrt{D}}{\sqrt{2}}\right)^t, \quad t \in \mathbb{N}, 2 \nmid t.$$

One can easily use Magma [4] to obtain the following result.

Lemma 2.3. *The equation*

$$X^2 - 5Y^4 = \pm 1, \quad X, Y \in \mathbb{N},$$

has only the solutions $(X, Y) = (2, 1)$ *and* $(9, 2)$.

The next result was obtained by Lebesgue [8].

Lemma 2.4. *The equation*

$$X^2 + 1 = Y^k, \quad X, Y, k \in \mathbb{N}, k > 1,$$

has no solution (X, Y, k).

Ke [7] proved a similar result.

Lemma 2.5. *The equation*

$$X^2 - 1 = Y^k, \quad X, Y, k \in \mathbb{N}, k > 1,$$

has only the solution $(X, Y, k) = (3, 2, 3)$.

We prove the next two results.

Lemma 2.6. *The equation*

$$X^2 + 1 = 2Y^k, \quad X, Y, k \in \mathbb{N}, X > 1, Y > 1, k > 2, \tag{2.3}$$

has only the solution $(X, Y, k) = (239, 13, 4)$.

Proof. We suppose that (X, Y, k) is a solution of (2.3). From a result in [16, see p. 168], we know that k has no odd prime factor, so we obtain $k = 2^r$, $r > 1$. From (2.3),

$$X^2 + 1 = 2(Y^{k/4})^4, \quad X, Y^{k/4} \in \mathbb{N}, X > 1, Y^{k/4} > 1. \tag{2.4}$$

From [9] we know that (2.4) has only the solutions $(X, Y^{k/4}) = (1, 1), (239, 13)$ and the proof of Lemma 2.6 is complete. □

Lemma 2.7. *The equation*

$$X^k + 1 = 2Y^2, \quad X, Y, k \in \mathbb{N}, X > 1, Y > 1, k > 2, \tag{2.5}$$

has only the solution $(X, Y, k) = (23, 78, 3)$.

Proof. We suppose that (X, Y, k) is a solution of (2.5). From [2, Theorem 1.1] with $n = k, y = 1, c = 2$, we know that $k < 4$. Multiplying $x^3 + 1 = 2y^2$ by 8 we obtain $Y^2 = X^3 + 8$, where $X = 2x$ and $Y = 4y$. Then we can use Magma [4] to obtain the following rational points:

$$(-2 : 0 : 1), (1 : 3 : 1), (2 : -4 : 1), (46 : 312 : 1),$$

whose corresponding solutions are

$$(x, y) = (1, 0), (\tfrac{1}{2}, \tfrac{3}{2}), (1, 1), (23, 78).$$

So the only solution of the equation $x^3 + 1 = 2y^2$, with $x > 1, y > 1$ is $(23, 78)$. This completes the proof of Lemma 2.7. □

The next result can be seen in [11, Section 15.2].

Lemma 2.8. *Let r be a positive odd number. All solutions of the equation*

$$X^2 + Y^2 = Z^{2^r}, \quad X, Y, Z \in \mathbb{N}, \gcd(X, Y) = 1, 2 \mid Y, \tag{2.6}$$

can be expressed as

$$X + Y\sqrt{-1} = \pm(a \pm b\sqrt{-1})^{2^r}, \quad Z = a^2 + b^2, \quad a, b \in \mathbb{N}, \quad \gcd(X, Y) = 1, 2 \mid ab.$$

Lemma 2.9. *Let t be a positive odd number. All solutions of the equation*

$$X^2 + Y^2 = 2Z^t, \quad X, Y, Z \in \mathbb{N}, \gcd(X, Y) = 1, \ 2 \nmid XY, \tag{2.7}$$

can be expressed as

$$\frac{X + Y\sqrt{-1}}{\sqrt{2}} = \pm\left(\frac{a \pm b\sqrt{-1}}{\sqrt{2}}\right)^t, \quad 2Z = a^2 + b^2, \quad a, b \in \mathbb{N}, \ \gcd(X, Y) = 1, \ 2 \nmid ab.$$

Proof. This is a special case of [20, Corollary 3.1], for $a = b = 1$ and $c = 2$. □

Lemma 2.10. *The system of equations*

$$X^2 - 2Y^2 = -1, \quad Z^2 - 3Y^2 = -2, \quad X, Y, Z \in \mathbb{N}, \tag{2.8}$$

has only the solution $(X, Y, Z) = (1, 1, 1)$.

Proof. If (2.8) has a solution (X, Y, Z) such that $(X, Y, Z) \neq (1, 1, 1)$, then X, Y, Z are three positive odd numbers satisfying $\min(X, Y, Z) \geq 3$ and $Z > Y$. From (2.8),

$$Y^2 + Z^2 = 2X^2, \quad \gcd(X, Z) = 1. \tag{2.9}$$

From (2.9),

$$\begin{gathered}\left(\frac{Z+Y}{2}\right)^2 + \left(\frac{Z-Y}{2}\right)^2 = X^2, \quad \frac{Z+Y}{2}, \frac{Z-Y}{2} \in \mathbb{N}, \\ \gcd\left(\frac{Z+Y}{2}, \frac{Z-Y}{2}\right) = 1, \quad 2 \,\Big|\, \left(\frac{Z+Y}{2}\right)\left(\frac{Z-Y}{2}\right).\end{gathered} \tag{2.10}$$

When $(Z - Y)/2$ is even, from Lemma 2.8 and (2.10),

$$\begin{gathered}\frac{Z+Y}{2} = a^2 - b^2, \quad \frac{Z-Y}{2} = 2ab, \quad X = a^2 + b^2, \\ a, b \in \mathbb{N}, a > b, \ \gcd(a, b) = 1, \ 2 \mid ab.\end{gathered} \tag{2.11}$$

Therefore,

$$X = a^2 + b^2, \quad Y = a^2 - 2ab - b^2. \tag{2.12}$$

From (2.12) and (2.8),

$$a^4 - 8a^3b + 2a^2b^2 + 8ab^3 + b^4 = 1.$$

Using Kant [6], one has $(a, b) = (0, \pm 1), (\pm 1, 0)$. This is impossible.

Similarly, when $(Z - Y)/2$ is odd, from (2.10) we know that

$$X = a^2 + b^2, \quad Y = -a^2 + 2ab + b^2,$$

where a, b satisfy (2.11). We come to the same conclusion. Thus (2.8) has only the solution $(X, Y, Z) = (1, 1, 1)$ and this completes the proof of Lemma 2.10. □

Lemma 2.11 [5, Theorem 1]. *The equation*

$$X^2 + 2 = 3^k, \quad X, k \in \mathbb{N},$$

has only the solutions $(X, k) = (1, 1)$ *and* $(5, 3)$.

Let α, β be two algebraic numbers. If $(\alpha + \beta)^2$ and $\alpha\beta$ are two nonzero coprime rational integers and α/β is not a root of unity, we call (α, β) a *Lehmer pair*. Suppose that $f = (\alpha + \beta)^2$, $g = \alpha\beta$. Then

$$\alpha = \tfrac{1}{2}(\sqrt{f} \pm \sqrt{h}), \quad \beta = \tfrac{1}{2}(\sqrt{f} \mp \sqrt{h}), \quad h = f - 4g.$$

The pair (f, h) is called the parameter of the Lehmer pair (α, β). For a positive integer k, one defines the corresponding sequence of *Lehmer numbers* by

$$L_k(\alpha,\beta) = \begin{cases} \dfrac{\alpha^k - \beta^k}{\alpha - \beta} & \text{when } 2 \nmid k, \\ \dfrac{\alpha^k - \beta^k}{\alpha^2 - \beta^2} & \text{when } 2 \mid k. \end{cases} \tag{2.13}$$

All Lehmer numbers are nonzero rational integers.

If two Lehmer pairs (α_1, β_1) and (α_2, β_2) satisfy $\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \{\pm 1, \pm\sqrt{-1}\}$, then we call them *equivalent*. When two Lehmer pairs (α_1, β_1) and (α_2, β_2) are equivalent, then $L_k(\alpha_1, \beta_1) = \pm L_k(\alpha_2, \beta_2)$, for $k \in \mathbb{N}$. When $k > 1$, a prime number p is a *primitive divisor* of $L_k(\alpha, \beta)$ if $p \mid L_k(\alpha, \beta)$ and $p \nmid (\alpha^2 - \beta^2)^2 L_1(\alpha, \beta) \cdots L_{k-1}(\alpha, \beta)$.

LEMMA 2.12 [19]. *When* $6 < k \le 30$ *and* $k \ne 8, 10, 12$, *if Lehmer numbers* $L_k(\alpha, \beta)$ *have no primitive divisor, then, equivalently, the parameters of the corresponding Lehmer pair* (α, β) *must be:*

(i) $k = 7$, $(f, h) = (1, -7), (1, -19), (3, -5), (5, -7), (13, -3), (14, -22)$;
(ii) $k = 9$, $(f, h) = (5, -3), (7, -1), (7, -5)$;
(iii) $k = 13$, $(f, h) = (1, -7)$;
(iv) $k = 14$, $(f, h) = (3, -13), (5, -3), (7, -1), (7, -5), (19, -1), (22, -14)$;
(v) $k = 15$, $(f, h) = (7, -1), (10, 2)$;
(vi) $k = 18$, $(f, h) = (1, -7), (3, -5), (5, -7)$;
(vii) $k = 24$, $(f, h) = (3, -5), (5, -3)$;
(viii) $k = 26$, $(f, h) = (7, -1)$;
(ix) $k = 30$, $(f, h) = (1, -7), (2, -10)$.

The following result is [3, Theorem 1.4].

LEMMA 2.13. *When* $k > 30$, *Lehmer numbers* $L_k(\alpha, \beta)$ *have primitive divisors.*

Properties 3.4 and 3.5 of [15] give the following lemma.

LEMMA 2.14. *If* p *is a primitive divisor of a Lehmer number* $L_q(\alpha, \beta)$, *where* q *is an odd prime, then* $p \equiv \pm 1 \pmod{2q}$.

3. Proof of Theorem 1.1

Suppose that (x, y, m, n) is a solution of (1.1). As p is an odd prime, x and y are positive odd numbers relatively prime to p.

When n is a power of 2, since $n > 2$,

$$n = 2^r, \quad r \in \mathbb{N}, r \ge 2. \tag{3.1}$$

From (1.1) and (3.1),

$$\left(\frac{x + p^m}{2}\right)^2 + \left(\frac{x - p^m}{2}\right)^2 = y^{2^r}, \tag{3.2}$$

where $(x+p^m)/2$ and $|x-p^m|/2$ are two coprime positive integers and one is odd and the other is even.

If $|x-p^m|/2$ is even, then from Lemma 2.8 and (3.2), we know that

$$\frac{x+p^m}{2}+\frac{|x-p^m|}{2}\sqrt{-1}=\pm(a\pm b\sqrt{-1})^{2^r}, \tag{3.3}$$

$$y=a^2+b^2, \quad a,b\in\mathbb{N}, \gcd(a,b)=1, 2\mid ab. \tag{3.4}$$

From (1.4), we know two rational integers $A(2^r,a,b)$ and $B(2^r,a,b)$ satisfying

$$A(2^r,a,b)+B(2^r,a,b)\sqrt{-1}=(a+b\sqrt{-1})^{2^r}, \tag{3.5}$$

so, from (3.3) and (3.5),

$$x=|A(2^r,a,b)\pm B(2^r,a,b)|, \quad p^m=|A(2^r,a,b)\mp B(2^r,a,b)|. \tag{3.6}$$

Similarly, if $|x-p^m|/2$ is odd, then, from (3.2),

$$\frac{|x-p^m|}{2}+\frac{x+p^m}{2}\sqrt{-1}=\pm(a\pm b\sqrt{-1})^{2^r} \tag{3.7}$$

and (3.4). From (3.5) and (3.7), we know that x and p^m also satisfy (3.6). So from (3.1), (3.4) and (3.5), we know that if p satisfies (1.5), then (1.1) has the solution (1.6) in case (ii).

If n is not a power of 2, then n must have an odd prime factor q and (1.1) can be rewritten as

$$x^2+(p^m)^2=2(y^{n/q})^q, \quad \gcd(x,p^m)=1. \tag{3.8}$$

From Lemma 2.9 and (3.8),

$$\frac{x+p^m\sqrt{-1}}{\sqrt{2}}=\pm\Big(\frac{a\pm b\sqrt{-1}}{\sqrt{2}}\Big)^q, \tag{3.9}$$

$$2y^{n/q}=a^2+b^2, \quad a,b\in\mathbb{N},\ \gcd(a,b)=1, 2\nmid ab. \tag{3.10}$$

Let

$$\alpha=\frac{a+b\sqrt{-1}}{\sqrt{2}}, \quad \beta=\frac{a-b\sqrt{-1}}{\sqrt{2}}. \tag{3.11}$$

Using (3.10) and (3.11), we know that both α and β are algebraic integers, $(\alpha+\beta)^2=2a^2$ and $\alpha\beta=y^{n/q}$ are two coprime positive integers, and

$$\frac{\alpha}{\beta}=\frac{\dfrac{a^2-b^2}{2}+ab\sqrt{-1}}{y^{n/q}}$$

is not a root of unity. Therefore, (α,β) is a Lehmer pair with the parameter $(2a^2,-2b^2)$. Suppose $L_k(\alpha,\beta)$, $k\in\mathbb{N}$, is the corresponding Lehmer number. Using (2.13), (3.9) and (3.11), we see that

$$p^m=b|L_q(\alpha,\beta)|. \tag{3.12}$$

We know that p is an odd prime and $L_q(\alpha, \beta)$ is a nonzero rational integer, so, from (3.12),

$$b = p^r, \quad r \in \mathbb{Z}, 0 \le r \le m. \tag{3.13}$$

If $r = 0$ then $b = 1$, and from (3.9) and (3.10) we obtain

$$x = |C(q, a)|,$$
$$p^m = |D(q, a)|,$$

and

$$a^2 + 1 = 2y^{n/q}. \tag{3.14}$$

If $n/q > 2$, from Lemma 2.6 and (3.14),

$$a = 239, \quad y = 13, \quad n = 4q.$$

If $n/q = 2$, (3.14) becomes

$$u^2 - 2v^2 = -1, \quad u, v \in \mathbb{N} \tag{3.15}$$

with $(u, v) = (a, y)$. Since the least solution of (3.15) is $(u_1, v_1) = (1, 1)$, from Lemma 2.1 we obtain

$$a = u(t), \quad y = v(t), \quad n = 2q,$$

where $u(t)$ and $v(t)$ satisfy (1.2).

If $n/q = 1$, (3.14) gives

$$y = \frac{a^2 + 1}{2}, \quad n = q, \quad a \in \mathbb{N}, a > 1, 2 \nmid a. \tag{3.16}$$

Therefore, if p satisfies (1.9) then (1.1) has the solution (1.10) in case (iv).

If $r > 0$ and $q > 5$, then from (3.12) and (3.13) we know that the Lehmer number $L_q(\alpha, \beta)$ has no primitive divisors by Lemmas 2.12 and 2.13 as the parameter is $(2a^2, -2b^2)$. So we will only consider the cases $r > 0$ and $q \in \{3, 5\}$.

If $0 < r < m$ and $q = 3$, then from (3.12) and (3.13) we know that $b = p^r$ and

$$p^{m-r} = \frac{|3a^2 - p^{2r}|}{2}. \tag{3.17}$$

As $\gcd(a, b) = 1$, using (3.17) we know that $p = 3$, $r = m - 1$, $b = 3^{m-1}$ and

$$a^2 + 2 = 3^{2m-3}. \tag{3.18}$$

Lemma 2.11 and (3.18) imply that $(a, m) = (1, 2)$ and $(5, 3)$. Therefore, we have the following two solutions of (1.1):

$$p = 3, \quad (x, y, m, n) = (13, 5, 2, 3), \ (545, 53, 3, 3). \tag{3.19}$$

If $r = m$ and $q = 3$, then (3.12) and (3.13) give $b = p^m$ and

$$p^{2m} - 3a^2 = -2. \tag{3.20}$$

Equation (3.20) can be transformed into the form

$$U^2 - 3V^2 = -2, \tag{3.21}$$

where $(U, V) = (p^m, a)$. We know that the least solution of (3.21) is $(U_1, V_1) = (1, 1)$. So Lemma 2.2 implies that

$$p^m = U(t), \quad a = V(t), \tag{3.22}$$

where $U(t)$ and $V(t)$ satisfy (1.3). Since $q = 3$, from (3.10) and (3.22), we deduce that

$$y^{n/3} = \frac{a^2 + b^2}{2} = \frac{V^2(t) + U^2(t)}{2} = 2V^2(t) - 1. \tag{3.23}$$

If $n/3 > 2$, then using Lemma 2.7 and (3.23), we get $a = V(t) = 78$. This contradicts (3.10) as a is an odd number. If $n/3 = 2$, then Lemma 2.10, (3.20), and (3.23) imply that $(X, Y, Z) = (y, V(t), a) = (1, 1, 1)$, which is impossible. So we have $n/3 = 1$. Therefore, from (3.9), (3.22) and (3.23), we know that if p satisfies (1.7), then (1.1) has the solution (1.8) in case (iii).

If $0 < r < m$ and $q = 5$, then we use (3.9), (3.12) and (3.13) to get $b = p^r$ and

$$p^{m-r} = \tfrac{1}{4}|5a^4 - 10a^2p^{2r} + p^{4r}|. \tag{3.24}$$

Since $\gcd(a, b) = 1$, (3.24) implies that $p = 5$, $r = m - 1$, $b = 5^{m-1}$ and

$$a^4 - 2 \cdot 5^{2m-2}a^2 + 5^{4m-5} = \pm 4. \tag{3.25}$$

From (3.25),

$$\left(\frac{a^2 - 5^{2m-2}}{2}\right)^2 - 5^{4m-5} = \pm 1.$$

As $m > 1$, $4m - 5 > 1$, then by Lemmas 2.4 and 2.5 this is impossible. Thus there is no solution when $0 < r < m$ and $q = 5$.

If $r = m$ and $q = 5$, then $b = p^m$ and we use the above method to obtain

$$5a^4 - 10a^2p^{2m} + p^{4m} = \pm 4,$$

that is,

$$\left(\frac{p^{2m} - 5a^2}{2}\right)^2 - 5a^4 = \pm 1. \tag{3.26}$$

We know that a is a positive odd number. Then Lemma 2.3 and (3.26) imply that $a = 1$ and $|p^{2m} - 5a^2| = |p^{2m} - 5| = 4$. Thus, $b = p^m = 3$. Using (3.9) and (3.10), we obtain the following solution of (1.1):

$$p = 3, \quad (x, y, m, n) = (79, 5, 1, 5). \tag{3.27}$$

So far we have obtained all solutions of (1.1) in cases (ii), (iii), and (iv). Finally, we will consider case (i). If $p = 3$, then from (3.19) and (3.27), we know that (1.1) has at least three solutions:

$$(x, y, m, n) = (13, 5, 2, 3), (545, 53, 3, 3), (79, 5, 1, 5). \tag{3.28}$$

If (1.1) has the solution (x, y, m, n) in case (ii), then as $3 \nmid xy$ and $n = 2^r$, by considerations modulo 3, (1.1) gives $x^2 + p^{2m} \equiv x^2 \equiv 1 \equiv 2 \equiv 2y^{2^r} \pmod 3$, which is a contradiction. If (1.1) has a solution in case (iii), then one can use (1.7) and (3.21) to get $0 \equiv p^{2s} \equiv U^2(t) \equiv 3V^2(t) - 2 \equiv -2 \pmod 3$, which is also a contradiction. If (1.1) has a solution in case (iv), then (1.9) implies that 3 is a primitive divisor of a Lehmer number $L_q(\alpha, \beta)$. So by Lemma 2.14, $3 \equiv \pm 1 \pmod{2q}$. This is impossible. Therefore, when $p = 3$, (1.1) has only the three solutions given in (3.28). This completes the proof of Theorem 1.1.

References

[1] F. S. Abu Muriefah, F. Luca, S. Siksek and S. Tengely, 'On the diophantine equation $x^2 + C = 2y^n$', *Int. J. Number Theory* **5**(6) (2009), 1117–1128.

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

[3] Y. Bilu, G. Hanrot and F. M. Voutier, 'Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte)', *J. reine angew. Math.* **539** (2001), 75–122.

[4] B. Wieb, C. John and P. Catherine, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24**(3–4) (1997), 235–265.

[5] Y. Bugeaud and T. N. Shorey, 'On the number of solutions of the generalized Ramanujan–Nagell equation', *J. reine angew. Math.* **539** (2001), 55–74.

[6] M. Daberkow, C. Fieker, J. Kluners, M. E. Pohst, K. Roegner and K. Wildanger, 'Kant V4', *J. Symbolic Comput.* **24** (1997), 267–283.

[7] Z. Ke, 'On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$', *Sci. Sinica* **14**(5) (1964), 457–460.

[8] V. A. Lebesgue, 'Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$', *Nouv. Ann. Math.* **9**(1) (1850), 178–181.

[9] W. Ljunggren, 'Zur theorie der Gleichung $x^2 + 1 = Dy^4$', *Det Norske Vid.-Akad. Avh. I.* **5** (1942), 27.

[10] W. Ljunggren, 'On the diophantine equation $Cx^2 + D = 2y^n$', *Math. Scand.* **18** (1966), 69–86.

[11] L. J. Mordell, *Diophantine Equations* (Academic Press, London, 1969).

[12] K. Petr, 'Sur l'équation de Pell', *Časopis Pest. Mat. Fys.* **56** (1927), 57–66 (in Czech).

[13] I. Pink, 'On the diophantine equation $x^2 + (p_1^{z_1} \cdots p_n^{z_n})^2 = 2y^n$', *Publ. Math. Debrecen* **65**(1–2) (2004), 205–213.

[14] I. Pink and S. Tengely, 'Full powers in arithmetic progressions', *Publ. Math. Debrecen* **57**(3–4) (2000), 535–545.

[15] P. Ribenboim, 'The Fibonacci numbers and the Arctic Ocean', in: *Symposia Gaussiana Conf. A* (Walter de Gruyter, Berlin, 1995), pp. 41–83.

[16] C. Störmer, 'L'équation $m \arctan(\frac{1}{x}) + n \arctan(\frac{1}{y}) = \frac{k\pi}{4}$', *Bull. Soc. Math. France* **27** (1899), 160–170.

[17] S. Tengely, 'On the diophantine equation $x^2 + a^2 = 2y^n$', *Indag. Math. (N.S.)* **15**(2) (2004), 291–304.

[18] S. Tengely, 'On the diophantine equation $x^2 + q^{2m} = 2y^p$', *Acta Arith.* **127**(1) (2007), 71–86.

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

[20] P.-Z. Yuan, 'On the diophantine equation $ax^2 + by^2 = ck^n$', *Indag. Math. (N.S.)* **16**(2) (2005), 301–320.

HUILIN ZHU, School of Mathematical Sciences, Xiamen University,
Xiamen 361005, PR China
e-mail: hlzhu@xmu.edu.cn

MAOHUA LE, Department of Mathematics, Zhanjiang Normal College,
Zhanjiang 524048, PR China
e-mail: lemaohua2008@163.com

ALAIN TOGBÉ, Department of Mathematics,
Purdue University North Central, 1401 S. U.S. 421, Westville, IN 46391, USA
e-mail: atogbe@pnc.edu