Period Math Hung (2017) 74:227–234
DOI 10.1007/s10998-016-0162-z

On the exponential Diophantine equation $(3pm^2 - 1)^x + (p(p-3)m^2 + 1)^y = (pm)^z$

Nobuhiro Terai[1] · **Takeshi Hibino**[2]

Published online: 7 November 2016

Abstract Let m be a positive integer, and let p be a prime with $p \equiv 1 \pmod 4$. Then we show that the exponential Diophantine equation $(3pm^2 - 1)^x + (p(p-3)m^2 + 1)^y = (pm)^z$ has only the positive integer solution $(x, y, z) = (1, 1, 2)$ under some conditions. As a corollary, we derive that the exponential Diophantine equation $(15m^2 - 1)^x + (10m^2 + 1)^y = (5m)^z$ has only the positive integer solution $(x, y, z) = (1, 1, 2)$. The proof is based on elementary methods and Baker's method.

Keywords Exponential Diophantine equation · Integer solution · Lower bound for linear forms in two logarithms

Mathematics Subject Classification 11D61

1 Introduction

Let a, b, c be fixed relatively prime positive integers greater than one. The exponential Diophantine equation

$$a^x + b^y = c^z \tag{1.1}$$

in positive integers x, y, z has been actively studied by a number of authors. This field has a rich history. Using elementary methods such as congruences, the quadratic reciprocity law and the arithmetic of quadratic (or cubic) fields, we can completely solve most of Eq. (1.1)

✉ Nobuhiro Terai
terai-nobuhiro@oita-u.ac.jp

Takeshi Hibino
hibino@toua-u.ac.jp

1 Department of Computer Science and Intelligent Systems, Faculty of Engineering, Oita University, 700 Dannoharu, Oita 870-1192, Japan

2 Department of Psychology and Child Studies, Faculty of Human Sciences, University of East Asia, 2-1 Ichinomiyagakuencho, Shimonoseki, Yamaguchi 751-8503, Japan

for small values of a, b, c. (cf. Nagell [16], Hadano [7] and Uchiyama [22].) It is known that the number of solutions (x, y, z) is finite, and all solutions can be effectively determined by means of Baker's method for linear forms in logarithms.

Jeśmanowicz [8] conjectured that if a, b, c are Pythagorean numbers, i.e., positive integers satisfying $a^2 + b^2 = c^2$, then (1.1) has only the positive integer solution $(x, y, z) = (2, 2, 2)$. As an analogue of Jeśmanowicz' conjecture, the first author proposed that if a, b, c, p, q, r are fixed positive integers satisfying $a^p + b^q = c^r$ with $a, b, c, p, q, r \geq 2$ and $\gcd(a, b) = 1$, then (1.1) has only the positive integer solution $(x, y, z) = (p, q, r)$ except for a handful of triples (a, b, c). These conjectures have been proved to be true in many special cases. They however, are still unsolved in general. (cf. [6,11,12,14,15,18,20]).

In the previous paper Terai [19], the first author showed that if m is a positive integer with $1 \leq m \leq 20$ or $m \not\equiv 3 \pmod 6$, then the Diophantine equation

$$(4m^2 + 1)^x + (5m^2 - 1)^y = (3m)^z \tag{1.2}$$

has only the positive integer solution $(x, y, z) = (1, 1, 2)$. The proof is based on elementary methods and Baker's method. Su-Li [17] proved that if $m \geq 90$ and $m \equiv 3 \pmod 6$, then Eq. (1.2) has only the positive integer solution $(x, y, z) = (1, 1, 2)$ by means of a result of Bilu–Hanrot–Voutier [3] concerning the existence of primitive prime divisors in Lucas-numbers. Recently, Bertók [1] has completely solved the remaining cases $20 < m < 90$ and $m \equiv 3 \pmod 6$ via the help of exponential congruences. (cf. Bertók-Hajdu [2].) In [13] and [21], we also showed that the Diophantine equations

$$(m^2 + 1)^x + (cm^2 - 1)^y = (am)^z \quad \text{with} \quad 1 + c = a^2,$$
$$(12m^2 + 1)^x + (13m^2 - 1)^y = (5m)^z$$

have only the positive integer solution $(x, y, z) = (1, 1, 2)$ under some conditions, respectively.

In this paper, we consider the exponential Diophantine equation

$$(3pm^2 - 1)^x + (p(p - 3)m^2 + 1)^y = (pm)^z \tag{1.3}$$

with m positive integer and p prime . Our main result is the following:

Theorem 1.1 *Let m be a positive integer with $m \not\equiv 0 \pmod 3$. Let p be a prime with $p \equiv 1 \pmod 4$. Moreover, suppose that if $m \equiv 1 \pmod 4$, then $p < 3784$. Then Eq. (1.3) has only the positive integer solution $(x, y, z) = (1, 1, 2)$.*

In particular, for $p = 5$, we can completely solve Eq. (1.3) without any assumption on m. The proof is based on applying a result on linear forms in p-adic logarithms due to Bugeaud [5] to Eq. (1.3) with $m \equiv 0 \pmod 3$.

Corollary 1.2 *The exponential Diophantine equation*

$$(15m^2 - 1)^x + (10m^2 + 1)^y = (5m)^z \tag{1.4}$$

has only the positive integer solution $(x, y, z) = (1, 1, 2)$.

2 Preliminaries

In order to obtain an upper bound for a solution y of Pillai's equation $c^z - b^y = a$ under some conditions, we need a result on lower bounds for linear forms in the logarithms of two algebraic numbers. We will introduce here some notations. Let α_1 and α_2 be real algebraic numbers with $|\alpha_1| \geq 1$ and $|\alpha_2| \geq 1$. We consider the linear form

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1,$$

where b_1 and b_2 are positive integers. As usual, the *logarithmic height* of an algebraic number α of degree n is defined as

$$h(\alpha) = \frac{1}{n}\left(\log |a_0| + \sum_{j=1}^{n} \log \max\left\{1, |\alpha^{(j)}|\right\}\right),$$

where a_0 is the leading coefficient of the minimal polynomial of α (over $\mathbb{Z}$) and $(\alpha^{(j)})_{1\leq j\leq n}$ are the conjugates of α. Let A_1 and A_2 be real numbers greater than 1 with

$$\log A_i \geq \max\left\{h(\alpha_i), \frac{|\log \alpha_i|}{D}, \frac{1}{D}\right\},$$

for $i \in \{1, 2\}$, where D is the degree of the number field $\mathbb{Q}(\alpha_1, \alpha_2)$ over $\mathbb{Q}$. Define

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

We choose to use a result due to Laurent [[10], Corollary 2] with $m = 10$ and $C_2 = 25.2$.

Proposition 2.1 (Laurent [10]) *Let Λ be given as above, with $\alpha_1 > 1$ and $\alpha_2 > 1$. Suppose that α_1 and α_2 are multiplicatively independent. Then*

$$\log |\Lambda| \geq -25.2\, D^4 \left(\max\left\{\log b' + 0.38, \frac{10}{D}\right\}\right)^2 \log A_1 \log\log A_2.$$

Next, we shall quote a result on linear forms in p-adic logarithms due to Bugeaud [5]. Here we consider the case where $y_1 = y_2 = 1$ in the notation from [5, p. 375].

Let p be an odd prime. Let a_1 and a_2 be non-zero integers prime to p. Let g be the least positive integer such that

$$\mathrm{ord}_p(a_1^g - 1) \geq 1, \quad \mathrm{ord}_p(a_2^g - 1) \geq 1,$$

where we denote the p-adic valuation by $\mathrm{ord}_p(\cdot)$. Assume that there exists a real number E such that

$$1/(p-1) < E \leq \mathrm{ord}_p(a_1^g - 1).$$

We consider the integer

$$\Lambda = a_1^{b_1} - a_2^{b_2},$$

where b_1 and b_2 are positive integers. We let A_1 and A_2 be real numbers greater than 1 with

$$\log A_i \geq \max\{\log |a_i|, E \log p\} \quad (i = 1, 2),$$

and we put $b' = b_1/\log A_2 + b_2/\log A_1$.

Proposition 2.2 (Bugeaud [5]) *With the above notation, if a_1 and a_2 are multiplicatively independent, then we have the upper estimate*

$$\mathrm{ord}_p(\Lambda) \leq \frac{36.1g}{E^3(\log p)^4}\left(\max\{\log b' + \log(E \log p) + 0.4, 6E \log p, 5\}\right)^2 \log A_1 \log A_2.$$

3 Proof of Theorem 1.1

In this section, we give a proof of Theorem 1.1.

Let (x, y, z) be a solution of (1.3). Taking (1.3) modulo p implies that $(-1)^x + 1 \equiv 0 \pmod{p}$. Hence x is odd.

3.1 The case where m is even

Using a congruence method, we ca easily show that if m is even, then Eq. (1.3) has only the positive integer solution $(x, y, z) = (1, 1, 2)$.

Lemma 3.1 *If m is even, then Eq.* (1.3) *has only the positive integer solution* $(x, y, z) = (1, 1, 2)$.

Proof If $z \leq 2$, then $(x, y, z) = (1, 1, 2)$ from (1.3). Hence we may suppose that $z \geq 3$. Taking (1.3) modulo m^3 implies that

$$-1 + 3pm^2x + 1 + p(p-3)m^2y \equiv 0 \pmod{m^3},$$

so

$$3px + p(p-3)y \equiv 0 \pmod{m},$$

which is impossible, since x is odd and m is even. We therefore conclude that if m is even, then Eq. (1.3) has only the positive integer solution $(x, y, z) = (1, 1, 2)$. □

3.2 The case where m is odd with $m \not\equiv 0 \pmod 3$

Lemma 3.2 *If m is odd with $m \not\equiv 0 \pmod 3$, then $x = 1$.*

Proof Suppose that $x \geq 2$. We show that this will lead to a contradiction. The proof is devided into two cases: Case 1: $m \equiv 1 \pmod 4$, Case 2: $m \equiv 3 \pmod 4$

Case 1: $m \equiv 1 \pmod 4$. Then, taking (1.3) modulo 4 implies that $3^y \equiv 1 \pmod 4$, so y is even.

On the other hand, taking (1.3) modulo 3, together with our assumption $m \not\equiv 0 \pmod 3$, implies that

$$(-1)^x + (-1)^y \equiv (pm)^z \not\equiv 0 \pmod 3, \tag{3.1}$$

which contradicts the fact that x is odd and y is even. Hence we obtain $x = 1$.

Case 2: $m \equiv 3 \pmod 4$. Then $\left(\frac{3pm^2-1}{p(p-3)m^2+1}\right) = 1$ and $\left(\frac{pm}{p(p-3)m^2+1}\right) = -1$, where $\left(\frac{*}{*}\right)$ denotes the Jacobi symbol. Indeed,

$$\left(\frac{3pm^2-1}{p(p-3)m^2+1}\right) = \left(\frac{3pm^2+p(p-3)m^2}{p(p-3)m^2+1}\right) = \left(\frac{p^2m^2}{p(p-3)m^2+1}\right) = 1$$

and

$$\begin{aligned}\left(\frac{pm}{p(p-3)m^2+1}\right) &= \left(\frac{p}{p(p-3)m^2+1}\right)\left(\frac{m}{p(p-3)m^2+1}\right)\\ &= -\left(\frac{p(p-3)m^2+1}{p}\right)\left(\frac{p(p-3)m^2+1}{m}\right)\\ &= -1,\end{aligned}$$

since $m \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 4$. In view of these, z is even from (1.3).

Taking (1.3) modulo 4 implies that $3^y \equiv (pm)^z \equiv 3^z \equiv 1 \pmod 4$, since z is even. Hence y is even. Similarly, (3.1) also leads to a contradiction. We therefore obtain $x = 1$. □

3.3 Pillai's equation $c^z - b^y = a$

From Lemma 3.2, it follows that $x = 1$ in (1.3), provided that m is odd with $m \not\equiv 0 \pmod 3$. If $y \leq 2$, then we obtain $y = 1$ and $z = 2$ from (1.3). From now on, we may suppose that $y \geq 3$. Hence our theorem is reduced to solving Pillai's equation

$$c^z - b^y = a \tag{3.2}$$

with $y \geq 3$, where $a = 3pm^2 - 1$, $b = p(p-3)m^2 + 1$ and $c = pm$.

We now want to obtain a lower bound for y.

Lemma 3.3 $y > m^2 - 2$.

Proof Since $y \geq 3$, Eq. (3.2) yields the following inequality:

$$(pm)^z \geq 3pm^2 - 1 + (p(p-3)m^2 + 1)^3 > (pm)^3.$$

Hence $z \geq 4$. Taking (3.2) modulo p^2m^4 implies that

$$3pm^2 - 1 + 1 + p(p-3)ym^2 \equiv 0 \pmod{p^2m^4},$$

so $3 + (p-3)y \equiv 0 \pmod{pm^2}$. Hence we have

$$y \geq \frac{1}{p-3}(pm^2 - 3) = \frac{p}{p-3}m^2 - \frac{3}{p-3} > m^2 - 2,$$

as desired. □

We next want to obtain an upper bound for y.

Lemma 3.4 $y < 2521 \log c$.

Proof From (3.2), we now consider the following linear form in two logarithms:

$$\Lambda = z \log c - y \log b \quad (>0).$$

Using the inequality $\log(1+t) < t$ for $t > 0$, we have

$$0 < \Lambda = \log\left(\frac{c^z}{b^y}\right) = \log\left(1 + \frac{a}{b^y}\right) < \frac{a}{b^y}. \tag{3.3}$$

Hence we obtain

$$\log \Lambda < \log a - y \log b. \tag{3.4}$$

On the other hand, we use Proposition 2.1 to obtain a lower bound for Λ. It follows from Proposition 2.1 that

$$\log \Lambda \;\geq\; -25.2 \left(\max\left\{\log b' + 0.38, 10\right\}\right)^2 (\log b)(\log c), \tag{3.5}$$

where $b' = \dfrac{y}{\log c} + \dfrac{z}{\log b}$.

We note that $b^{y+1} > c^z$. Indeed,

$$b^{y+1} - c^z = b(c^z - a) - c^z = (b-1)c^z - ab \geq p(p-3)m^2 \cdot p^2m^2 - (3pm^2 - 1)(p(p-3)m^2 + 1) > 0.$$

Hence $b' < \dfrac{2y+1}{\log c}$.

Put $M = \dfrac{y}{\log c}$. Combining (3.4) and (3.5) leads to

$$y \log b < \log a + 25.2 \left(\max \left\{ \log \left(2M + \frac{1}{\log c} \right) + 0.38,\ 10 \right\} \right)^2 (\log b)\,(\log c),$$

so

$$M < 1 + 25.2\ (\max \{\log (2M+1) + 0.38,\ 10\})^2,$$

since $\log c = \log(pm) \geq \log 5 > 1$. We therefore obtain $M < 2521$. This completes the proof of Lemma 3.4. □

We are now in a position to prove Theorem 1.1. It follows from Lemmas 3.3, 3.4 that

$$m^2 - 2 < 2521 \log(pm). \tag{3.6}$$

We want to obtain an upper bound for p and then one for m. We first show that if $m \equiv 3 \pmod 4$, then $p < 3784$. Recall that z is even for the case $m \equiv 3 \pmod 4$, as seen in the proof of Lemma 3.2. Put $z = 2Z$ with Z positive integer. Now Eq. (3.2) can be written as

$$(c^2)^Z - b^y = c^2 - b.$$

Then $y \geq Z$. If $y = Z$, then we obtain $y = Z = 1$. If $y > Z$, then we consider a "gap" between the trivial solution $(y, Z) = (1, 1)$ and (possibly) another solution (y, Z).

From $a + b = c^2$ and $a + b^y = c^{2Z}$, consider the following two linear forms in two logarithms:

$$\Lambda_0 = 2 \log c - \log b\ (> 0), \quad \Lambda = 2Z \log c - y \log b\ (> 0).$$

Then

$$y\Lambda_0 - \Lambda = 2(y - Z) \log c \geq 2 \log c,$$

so

$$y > \frac{2}{\Lambda_0} \log c.$$

By Lemma 3.4, we have $\dfrac{2}{\Lambda_0} \log c < 2512 \log c$. Hence

$$\frac{2}{2521} < \Lambda_0 = \log \left(\frac{c^2}{b} \right) = \log \left(1 + \frac{a}{b} \right) < \frac{a}{b} = \frac{3pm^2 - 1}{p(p-3)m^2 + 1} < \frac{3pm^2}{p(p-3)m^2}$$
$$= \frac{3}{p-3}.$$

Consequently we obtain $p < 3784$. When $m \equiv 1 \pmod 4$,we could not prove that z is even in Lemma 3.2. We therefore suppose that if $m \equiv 1 \pmod 4$, then $p < 3784$. In any case, (3.6) yields $m \leq 183$.

From (3.3), we have the inequality

$$\left| \frac{\log b}{\log c} - \frac{z}{y} \right| < \frac{a}{y b^y \log c},$$

which implies that $\left|\frac{\log b}{\log c} - \frac{z}{y}\right| < \frac{1}{2y^2}$, since $y \geq 3$. Thus $\frac{z}{y}$ is a convergent in the simple continued fraction expansion to $\frac{\log b}{\log c}$.

On the other hand, if $\frac{p_r}{q_r}$ is the r-th such convergent, then

$$\left|\frac{\log b}{\log c} - \frac{p_r}{q_r}\right| > \frac{1}{(a_{r+1}+2)q_r^2},$$

where a_{r+1} is the $(r+1)$-st partial quotient to $\frac{\log b}{\log c}$ (see e.g. Khinchin [9]). Put $\frac{z}{y} = \frac{p_r}{q_r}$. Note that $q_r \leq y$. It follows, then, that

$$a_{r+1} > \frac{b^y \log c}{ay} - 2 \geq \frac{b^{q_r} \log c}{aq_r} - 2. \tag{3.7}$$

Finally, we checked by Magma [4] that for each $p < 3784$ with $p \equiv 1 \pmod 4$, inequality (3.7) does not hold for any r with $q_r < 2521 \log(pm)$ in the range $3 \leq m \leq 183$. This completes the proof of Theorem 1.1.

4 Proof of Corollary 1.2

Let (x, y, z) be a solution of (1.4). By Theorem 1.1, we may suppose that $m \equiv 0 \pmod 3$. Recall that x is odd. Here, we apply Proposition 2.2. For this, we set $p := 3$, $a_1 := 10m^2 + 1$, $a_2 := 1 - 15m^2$, $b_1 := y$, $b_2 := x$, and

$$\Lambda := (10m^2+1)^y - (1-15m^2)^x.$$

Then we may take $g = 1$, $E = 2$, $A_1 = 10m^2 + 1$, $A_2 := 15m^2 - 1$. Hence we have

$$z \leq \frac{36.1}{8(\log 3)^4}\left(\max\{\log b' + \log(2\log 3) + 0.4,\ 12\log 3\}\right)^2 \log(10m^2+1)\log(15m^2-1),$$

where $b' := \frac{y}{\log(15m^2-1)} + \frac{x}{\log(10m^2+1)}$. Suppose that $z \geq 4$. We will observe that this leads to a contradiction. Taking (1.4) modulo m^4, we find

$$15x + 10y \equiv 0 \pmod{m^2}.$$

In particular, we find $M := \max\{x, y\} \geq m^2/25$. Therefore, since $z \geq M$ and $b' \leq \frac{M}{\log m}$, we find

$$M \leq 3.1\left(\max\left\{\log\left(\frac{M}{\log m}\right) + \log(2\log 3) + 0.4,\ 12\log 3\right\}\right)^2 \log(10m^2+1)\log(15m^2-1). \tag{4.1}$$

If $m \geq 3450$, then

$$M \leq 3.1\left(\log\left(\frac{M}{\log m}\right) + \log(2\log 3) + 0.4\right)^2 \log(10m^2+1)\log(15m^2-1).$$

Since $m^2 \leq 25M$, the above inequality gives

$$M \leq 3.1\,(\log M - \log(\log 3450) + 1.19)^2 \log(250M+1)\log(375M-1).$$

We therefore obtain $M \leq 105186$, which contradicts the fact that $M \geq m^2/25 \geq 476100$.

If $m < 3450$, then inequality (4.1) gives

$$\frac{m^2}{25} \leq 539 \log(10m^2 + 1) \log(15m^2 - 1).$$

This implies $m \leq 2062$. Hence all x, y and z are also bounded. It is not hard to verify by Magma [4] that there is no (m, x, y, z) under consideration satisfying (1.4). We conclude $z \leq 3$. In this case, one can easily show that $(x, y, z) = (1, 1, 2)$. This completes the proof of Corollary 1.2.

Remark In the same way as in the proof of Corollary 1.2, we can completely solve "the remaining case" $m \equiv 0 \pmod 3$ of Eq. (1.2), which is shown by Su-Li [17] and Bertók [1].

Acknowledgements The first author is supported by JSPS KAKENHI Grant (No. 15K04786).

References

1. C. Bertók, The complete solution of the Diophantine equation $(4m^2+1)^x+(5m^2-1)^y = (3m)^z$. Period. Math. Hung. **72**, 37–42 (2016)
2. C. Bertók, L. Hajdu, A Hasse-type principle for exponential Diophantine equations and its applications. Math. Comput. **85**, 849–860 (2016)
3. Y. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers. Journal für die Reine und Angewandte Mathematik **539**, 75–122 (2001)
4. W. Bosma, J. Cannon, *Handbook of Magma Functions* (Department of Mathematics, University of Sydney), http://magma.maths.usyd.edu.au/magma/
5. Y. Bugeaud, Linear forms in p-adic logarithms and the Diophantine equation $(x^n - 1)/(x - 1) = y^q$. Math. Proc. Camb. Philos. Soc. **127**, 373–381 (1999)
6. Z. Cao, A note on the Diophantine equation $a^x + b^y = c^z$. Acta Arith. **91**, 85–93 (1999)
7. T. Hadano, On the Diophantine equation $a^x = b^y + c^z$. Math. J. Okayama Univ. **19**, 1–5 (1976)
8. L. Jeśmanowicz, Some remarks on Pythagorean numbers. Wiadom. Mat. **1**, 196–202 (1955/1956) **(in Polish)**
9. A.Y. Khinchin, *Continued Fractions*, 3rd edn. (P. Noordhoff Ltd., Groningen, 1963)
10. M. Laurent, Linear forms in two logarithms and interpolation determinants II. Acta Arith. **133**, 325–348 (2008)
11. T. Miyazaki, Terai's conjecture on exponential Diophantine equations. Int. J. Number Theory **7**, 981–999 (2011)
12. T. Miyazaki, Generalizations of classical results on Jeśmanowicz' conjecture concerning primitive Pythagorean triples. J. Number Theory **133**, 583–595 (2013)
13. T. Miyazaki, N. Terai, On the exponential Diophantine equation $(m^2+1)^x+(cm^2-1)^y = (am)^z$. Bull. Aust. Math. Soc. **90**, 9–19 (2014)
14. T. Miyazaki, N. Terai, On Jeśmanowicz' conjecture concerning primitive Pythagorean triples II. Acta Math. Hungarica **147**, 286–293 (2015)
15. T. Miyazaki, P. Yuan, D. Wu, Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples II. J. Number Theory **141**, 184–201 (2014)
16. T. Nagell, Sur une classe d'équations exponentielles. Ark. Mat. **3**, 569–582 (1958)
17. J. Su, X. Li, The exponential Diophantine equation $(4m^2 + 1)^x + (5m^2 - 1)^y = (3m)^z$. Abstr. Appl. Anal. **2014**, 1–5 (2014)
18. N. Terai, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations. Acta Arith. **90**, 17–35 (1999)
19. N. Terai, On the exponential Diophantine equation $(4m^2 + 1)^x + (5m^2 - 1)^y = (3m)^z$. Int. J. Algebra **6**, 1135–1146 (2012)
20. N. Terai, On Jeśmanowicz' conjecture concerning primitive Pythagorean triples. J. Number Theory **141**, 316–323 (2014)
21. N. Terai, T. Hibino, On the exponential Diophantine equation $(12m^2+1)^x+(13m^2-1)^y = (5m)^z$. Int. J. Algebra **9**, 261–272 (2015)
22. S. Uchiyama, On the Diophantine equation $2^x = 3^y + 13^z$. Math. J. Okayama Univ. **19**, 31–38 (1976)