Journal of Algebra, Number Theory: Advances and Applications
Volume 4, Number 2, 2010, Pages 91-103

ON THE DIOPHANTINE EQUATION $3^{2n} - 2 \cdot 3^m + 1 = k^2$

GERVASIO G. BASTOS and DIEGO MARQUES

Departamento de Matemática
Universidade Estadual do Ceará
Ceará, CEP: 60740-903
Brazil

Departamento de Matemática
Universidade de Brasília
Brasília, CEP: 70910-900
Brazil
e-mail: diego@mat.unb.br

Abstract

In 1981, Beukers used a hypergeometric method for proving that the well-known generalized Ramanujan-Nagell equation

$$x^2 + C = p^n, \; p \text{ prime},$$

has at most one solution in positive integers x and n, where C and p are previously fixed, with a few exceptions.

In this note, we give an elementary proof of this result when n is even as well as the complete solution of a such equation when C is a power of 2009. Moreover, we prove that the previous result is surprisingly connected with the title equation, which allow us to find all solutions for that equation.

2010 Mathematics Subject Classification: Primary 11D61; Secondary 11J86.

Keywords and phrases: Diophantine equation, linear forms in logarithms, Baker-Davenport, Ramanujan-Nagell.

Received November 27, 2010

1. Introduction

The Diophantine equation

$$x^2 + C = y^n, \quad x \geq 1, \quad y \geq 1, \quad n \geq 3, \tag{1.1}$$

has a rich history and it has attracted the attention of several mathematicians. Several papers have been written on this topic, specially for particular values of C. The first non-trivial result is due to Lebesgue [21] and date back to the 1850. He proved that the above equation has no solutions for $C = 1$. In 1965, Ko [18] proved that if $C = -1$, then the only solution is $(x, y, n) = (3, 2, 3)$. In 2004, Tengely [31] solved the above equation with $C = B^2$ and $B \in \{3, 4, \ldots, 501\}$. The case when $C = p^k$, where p is a prime number, was studied for $p = 2$, in [5, 19, 20], for $p = 3$ in [6, 7, 22], for $p = 5$ in [1, 2] and for $p = 7$ in [24]. Some advances on an arbitrary prime p appear in [8]. The equations $x^2 + C = y^n$ with $1 \leq C \leq 100$ were completely solved in [12]. Also, the solutions when x and y are coprime $C = 2^a \cdot 3^b, C = 2^a \cdot 5^b$, and $C = 5^a \cdot 13^b$ can be found in [3, 23, 25], respectively. The more recent progress on the subject concerns to cases $C = 5^a \cdot 11^b, C = 2^a \cdot 11^b$, $C = 2^a \cdot 3^b \cdot 11^c$, can be found in [13, 14, 15].

Also, several authors become interested in Equation (1.1) when the variable y is replaced by a positive integer number. The equation

$$x^2 + C = t^n,$$

where C and t are given integers, is called the *generalized Ramanujan-Nagell equation*. For instance, there is quite an extensive literature concerning the equation

$$x^2 + C = p^n, \quad p \text{ prime}, \tag{1.2}$$

beginning for the case $C = 7$ and $p = 2$, which was posed in a work of Ramanujan [28, 29], in 1913 and first solved by Nagell [27] in 1948. The case $C = 11$ and $p = 3$ was treated by Cohen [16] in 1976. Consult its very extensive annotated bibliography for additional references and history. As a final remark, we point out that, in 1960, Apéry [4] showed that Equation (1.2), when $p \nmid C$, has at most two solutions.

Here, we are particularly interested in solving the Diophantine equation

$$3^{2n} - 2 \cdot 3^{m} + 1 = k^{2}. \tag{1.3}$$

We prove that the possible solutions for the above equation are related to the solubility of the generalized Ramanujan-Nagell equation for $t = 9$. Our first result is the following:

Theorem 1.1. *Let C be a positive integer. Then the Diophantine equation*

$$x^{2} + C = 3^{2n}, \tag{1.4}$$

has at most one solution in positive integers x and n.

It is important to pay attention that Equation (1.4) has solution only when $C \equiv 0, 2 \pmod 3$.

After, we shall combine two powerful techniques in number theory, namely, the Baker's theory on linear forms in logarithms and some tools from Diophantine approximation, due to Baker and Davenport to find a general method for solving Equation (1.4) for values of C previously fixed. As application of it, we derive the following:

Theorem 1.2. *The Diophantine equation*

$$x^{2} + 2009^{t} = 3^{2n}, \tag{1.5}$$

has no solution in positive integers x, t, and n.

Finally, we prove:

Theorem 1.3. *The only solutions of the Diophantine equation*

$$3^{2n} - 2 \cdot 3^{m} + 1 = k^{2},$$

in positive integers m, n, and k, are those related to $m = n$, i.e., $(n, m, k) = (n, n, 3^{n} - 1)$.

We point out that our method is quite general and can be applied by replacing 3 in the title equation by any odd prime number p.

2. The Diophantine Equation $x^2 + C = 3^{2n}$

2.1. The proof of Theorem 1.1

It is important to get noticed that Beukers [10, 11] proved that Equation (1.2) (and consequently, Equation (1.4)) has at most one solution except when $(p, C) = (3, 2)$ or $(4t^2 + 1, 3t^2 + 1)$, for a positive t. In all these exceptional cases, the pair $(x, n) = (1, 1)$ is a direct solution and so Theorem 1.1 is according to Beukers result. He used refined techniques on hypergeometric methods for proving these results.

Here, we will present an elementary demonstration of the Theorem 1, which was discovered by Professor F. A. Germano who has communicated us his nice proof by e-mail.

Proof. Suppose that x, y, m, and n are positive integer numbers such that $x^2 + C = 3^{2m}$ and $y^2 + C = 3^{2n}$. We shall show that $m = n$ and consequently, $x = y$. First of all, we note that

$$(3^m + x)(3^m - x) = C = (3^n + y)(3^n - y).$$

Without losing any generality, we can suppose $\gcd(C, 3) = \gcd(x, 3) = 1$. In fact, we have $x = 3^u a$, $C = 3^v b$, where $a, b \in \mathbb{N}$, $3 \nmid ab$, u and v are nonnegative integer numbers. Hence

$$x^2 + C = 3^{2u} a^2 + 3^v b = 3^{2m}.$$

Of course, $2m \geq \max\{2u, v\}$. Set $\ell = \min\{2u, v\}$, we have $\ell \leq 2u, v \leq 2m$ and $3^\ell (3^{2u-\ell} a^2 + 3^{v-\ell} b) = 3^{2m}$. We then conclude that either $2u = \ell = v$ or $3 \nmid (3^{2u-\ell} a^2 + 3^{v-\ell} b)$. In the first case, we have

$$a^2 + b = 3^{2(m-u)}, \tag{2.1}$$

with $m - u > 0$ and whence it is enough to prove the theorem for Equation (2.1). In the second case, we infer that $1 = 3^{2u-t}a^2 + 3^{v-t}b > 1$, which is absurd.

We have then $C = (3^m - x)(3^m + x) = r(2 \cdot 3^m - r)$, where $0 < r = 3^m - x < 3^m$. Thus, if (x, m) is a solution of (1.4), we get an integer number $0 < r < 3^m$ such that $C = r(2 \cdot 3^m - r)$ and $3 \nmid r$. Therefore, for another solution (y, n) of (1.4), there exists $0 < s = 3^n - y < 3^n$ such that $C = s(2 \cdot 3^n - s)$ and $3 \nmid s$.

We claim that $m = n$. Towards a contradiction, we may suppose $n > m$ (the other case can be handled in much the same way). This implies that $0 < s < r < 3^m$. Indeed, if $r \leq s$, then $2 \cdot 3^m - r < 2 \cdot 3^m < 3^{m+1} \leq 3^n$, yielding

$$C = r(2 \cdot 3^m - r) < r \cdot 3^n \leq s \cdot 3^n < s(2 \cdot 3^n - s) = C,$$

which is a contradiction.

Also, the relation $s(2 \cdot 3^n - s) = r(2 \cdot 3^m - r)$ implies that r and s have the same parity, since $s^2 \equiv r^2 \pmod 2$. By considerations modulo 3^m, it is easy to deduce that $s^2 \equiv r^2 \pmod{3^m}$ and so $3^m | (r - s)(r + s)$. Recall that the numbers $r - s$ and $r + s$ cannot be both multiples of 3 (otherwise $3 | r$ and $3 | s$). It follows that $r \equiv \pm s \pmod{3^m}$, which yields

$$r \pm s \in \{\dots, -3^{m+1}, -2 \cdot 3^m, -3^m, 0, 3^m, 2 \cdot 3^m, 3^{m+1}, \dots\} = 3^m \mathbb{Z}.$$

Since $0 < s < r < 3^m$, we get $0 < r \pm s < 2 \cdot 3^m$ and therefore, $r \pm s = 3^m$, but this is absurd because $r \pm s$ is even (keep in mind that r and s have the same parity). Thus $m = n$ as desired.

$\square$

2.2. The proof of Theorem 1.2

2.2.1. Auxiliary results

Before proceeding further, we recall some results, which will be very useful in what follows.

The main idea for proving the Theorem 1.2 is to use bounds *à la Baker* for a suitable linear form in three logarithms and then to deduce an upper bound on t. From the main result of Matveev [26], we extract the following result:

Lemma 1. *Let* $\alpha_1, \alpha_2, \alpha_3$ *be real algebraic numbers and let* b_1, b_2, b_3 *be nonzero integer rational numbers. Define*

$$\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + b_3 \log \alpha_3.$$

Let D *be the degree of the number field* $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ *over* $\mathbb{Q}$ *and let* A_1, A_2, A_3 *be real numbers, which satisfy*

$$A_j \geq \max\{Dh(\alpha_j), |\log \alpha_j|, 0.16\}, \text{ for } j = 1, 2, 3.$$

Assume that

$$B \geq \max\{1, \max\{|b_j| A_j / A_1; 1 \leq j \leq 3\}\}.$$

Define also

$$C_1 = 6750000 \cdot e^4 (20.2 + \log(3^{5.5} D^2 \log(eD))).$$

If $\Lambda \neq 0$, *then*

$$\log|\Lambda| \geq -C_1 D^2 A_1 A_2 A_3 \log(1.5eDB \log(eD)).$$

As usual, in the previous statement, the *logarithmic height* of an s-degree algebraic number α is defined as

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

where a is the leading coefficient of the minimal polynomial of α (over $\mathbb{Z}$) and $(\alpha^{(j)})_{1 \leq j \leq s}$ are the conjugates of α.

After finding an upper bound on t, which is general too large, the next step is to reduce it. For this purpose, we need a variant of the famous Baker-Davenport lemma, which is due to Dujella and Pethö [17]. For a real number x, we use $\| x \| = \min\{|x - n| : n \in \mathbb{N}\}$ for the distance from x to the nearest integer.

Lemma 2. *Suppose that* M *is a positive integer. Let* p/q *be a convergent of the continued fraction expansion of the irrational number* γ *such that* $q > 6M$, *and let* $\epsilon = \| \mu q \| - M \| \gamma q \|$, *where* μ *is a real number. If* $\epsilon > 0$, *then there is no solution to the inequality*

$$0 < m\gamma - n + \mu < A \cdot B^{-m},$$

in positive integers m, n *with*

$$\frac{\log(Aq/\epsilon)}{\log B} \leq m < M.$$

See Lemma 5 (a) in [17].

Now, we are ready to deal with the proof of our result.

2.2.2. The proof

Finding a bound on *k*. First, note that t in Equation (1.5) must be odd, say $2k + 1$, because $x^2 \equiv 0, 1 \pmod 3$ and $2009 \equiv -1 \pmod 3$. So, Equation (1.5) can be rewritten in the form:

$$2009^{2k+1} = (3^n - x)(3^n + x). \tag{2.2}$$

Since $3 \nmid x$ (because $3 \nmid 2009$), we get

$$\{3^n - x, 3^n + x\} = \{1, 2009^{2k+1}\} \text{ or } \{41^{2k+1}, 49^{2k+1}\},$$

which leads to equations

$$2 \cdot 3^n - 2009^{2k+1} = 1, \tag{2.3}$$

or

$$2 \cdot 3^n - 49^{2k+1} = 41^{2k+1}. \tag{2.4}$$

Here, we shall work only on the Equation (2.3). The proof that Equation (2.4) has no solution proceeds along the same lines.

We point out that Equation (2.3) has no solution when $n = 2k + 1$ even, if we replace 3 by any arbitrary prime number p. This fact is an immediate consequence of a result due to Bennett [9]. For any positive integer a, the equation

$$(a+1)x^n - ay^n = 1, \text{ in integers } x \geq 1,\ y \geq 1,\ n \geq 3,$$

has no solution other than given by $x = y = 1$.

For the remaining cases $(n \neq 2k+1)$, we shall use bounds for linear forms in three logarithms of algebraic numbers (for more details on transcendental methods to Diophantine equations, we refer the reader to [30]).

First, on dividing Equation (2.3) through by 2009^{2k+1}, we get

$$2 \cdot 3^n \cdot 2009^{-(2k+1)} - 1 = 2009^{-(2k+1)}.$$

Let $\Lambda = (2k+1)\log(1/2009) - n\log(1/3) + \log 2$, then the previous equality becomes $e^{\Lambda} - 1 = 2009^{-(2k+1)} > 0$ and so $\Lambda > 0$. Therefore, $\Lambda < e^{\Lambda} - 1 = 2009^{-(2k+1)}$, which yields

$$\log \Lambda < -(2k+1)\log 2009. \tag{2.5}$$

Now, we will apply Lemma 1. Take

$$\alpha_1 = 1/2009,\ \alpha_2 = 1/3,\ \alpha_3 = 2,\ b_1 = 2k+1,\ b_2 = -n,\ b_3 = 1.$$

Observe that $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}$ and then $D = 1$. Surely, we can take $A_1 = \log 2009$, $A_2 = \log 3$, and $A_3 = \log 2$.

Note that

$$\max\{1, \max\{|b_j|A_j / A_1;\ 1 \leq j \leq 3\}\} = \max\{2k+1,\ n\log 3/\log 2009\},$$

and then it suffices to choose $B = 2k+1$ as

$$2 \cdot 3^n = 2009^{2k+1} + 1 < 2 \cdot 2009^{2k+1}, \text{ and then } n\log 3 < (2k+1)\log 2009.$$

Since, for $D = 1$, it holds that $C_1 < 9.7 \cdot 10^9$, Lemma 1 yields

$$\log|\Lambda| > -56.2 \cdot 10^9 \log(4.08(2k+1)). \tag{2.6}$$

Combining the estimates (2.5) and (2.6), we get

$$56.2 \cdot 10^9 \log(4.08(2k+1)) > (2k+1)\log 2009,$$

and this inequality implies $k < 2 \cdot 10^{11}$ (for the sake of preciseness $k < 101389315227$).

Reducing the bound. Since $0 < \Lambda < 2009^{-2k-1}$, we have that

$$0 < (2k+1)\log \alpha_1 - n\log \alpha_2 + \log \alpha_3 < 2009^{-2k}.$$

On dividing through by $\log \alpha_2$, we get

$$0 < (2k+1)\gamma - n + \mu < 2009^{-2k}, \tag{2.7}$$

with $\gamma = \log \alpha_1 / \log \alpha_2$ and $\mu = \log \alpha_3 / \log \alpha_2$.

Surely, γ is an irrational number[1] (because 2009 and 3 are multiplicatively independent). So, let us denote p_ℓ / q_ℓ be the ℓ-th convergent of its continued fraction.

In order to reduce our bound on k (which is too large!), we will use the Lemma 2.

For that, take $M = 2 \cdot 10^{11}$. Since

$$\frac{p_{27}}{q_{27}} = \frac{24782374449400}{3579857528251},$$

then $q_{27} \geq 3579857528251 > 1.2 \cdot 10^{12} = 6M$. Moreover, a straight calculation gives

[1]Actually, this number is transcendental by Gelfond-Schneider theorem: If α and β are algebraic numbers, with $\alpha \neq 0$ or 1, and β is irrational, then α^β is transcendental.

$$M\| q_{27}\gamma \| = 0.02760\ldots < 0.03,$$

and

$$\| q_{27}\mu \| = 0.33016\ldots > 0.33.$$

Hence

$$\epsilon = \| \mu q_{27} \| - M\| \gamma q_{27} \| > 0.33 - 0.03 = 0.3.$$

Thus, all the hypotheses of the Lemma 2 are satisfied with $A = 1$ and $B = 2009^2$. It follows from that lemma that there is no solution of the Diophantine equation (2.2) in the range

$$\left[\left\lfloor \frac{\log(Aq_{27} / \epsilon)}{\log B} \right\rfloor + 1,\ M\right] = [2,\ 2 \cdot 10^{11}].$$

Thus $k = 1$, which is absurd, since 4054243365 is not a power of 3. This completes the proof. □

3. The Proof of Theorem 1.3

Note that if $m = n$, then $3^{2n} - 2 \cdot 3^n + 1 = (3^n - 1)^2$. If k is positive, then $(n, m, k) = (n, n, 3^n - 1)$ is solution for (1.3) for all positive integer n. Our goal is to prove that this one is the only possibility.

For that, in order to facilitate our work, we shall denote $\delta_{m,n} = 3^{2n} - 2 \cdot 3^m + 1$, and let m, n, k be positive integer numbers such that $\delta_{m,n} = k^2$. First, take $p = 3^n + k$ and $q = 3^n - k$. So, we have $p > q \geq 1$, $p + q = 2 \cdot 3^n$ and $pq = 2 \cdot 3^m - 1$. Now, if $x = 3^m - 1$ and $y = 3^n - q = k$, we get

$$x = 3^m - 1 = pq - 3^m \text{ and } y = 3^n - q = p - 3^n = k,$$

yielding

$$(3^m + x)(3^m - x) = pq = (3^n + y)(3^n - y).$$

Thus (x, n) and (y, m) are solutions of Equation (1.4) with $C = pq$. Hence, we apply the Theorem 1.1 to get $m = n$ and this completes our proof. $\square$

Acknowledgement

The authors would like to express their gratitude to Francisco Germano and Alain Togbé by their very nice suggestions.

References

[1] F. S. Abu Muriefah and S. A. Arif, The Diophantine equation $x^2 + 5^{2k+1} = y^n$, Indian J. Pure Appl. Math. 30 (1999), 229-231.

[2] F. S. Abu Muriefah, On the Diophantine equation $x^2 + 5^{2k} = y^n$, Demonstratio Math. 39 (2006), 285-289.

[3] F. S. Abu Muriefah, F. Luca and A. Togbé, On the Diophantine equation $x^2 + 5^a \cdot 13^b = y^n$, Glasgow Math. J. 50 (2006), 175-181.

[4] R. Apéry, Sur une équation diophantienne, C. R. Acad. Sci. Paris Sér. A 251 (1960), 1263-1264 and 1451-1452.

[5] S. A. Arif and F. S. Abu Muriefah, On the Diophantine equation $x^2 + 2^k = y^n$, Int. J. Math. Math. Sci. 20 (1997), 299-304.

[6] S. A. Arif and F. S. Abu Muriefah, On the Diophantine equation $x^2 + 3^m = y^n$, Int. J. Math. Math. Sci. 21 (1998), 619-620.

[7] S. A. Arif and F. S. Abu Muriefah, On a Diophantine equation, Bull. Austral. Math. Soc. 57 (1998), 189-198.

[8] S. A. Arif and F. S. Abu Muriefah, On the Diophantine equation $x^2 + q^{2k+1} = y^n$, J. Number Theory 95 (2002), 95-100.

[9] M. A. Bennett, Rational approximation to algebraic numbers of small height: The Diophantine equation $|ax^n - by^n| = 1$, Jour. Reine Angew. Math. 535 (2001), 1-49.

[10] F. Beukers, On the generalized Ramanujan-Nagell equations, I, Acta Arith. 38 (1980/1981), 389-410.

[11] F. Beukers, On the generalized Ramanujan-Nagell equations, II, Acta Arith. 39 (1981), 113-123.

[12] Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches to exponential Diophantine equations, II, The Lebesgue-Nagell equation, Compositio Math. 142 (2006), 31-62.

[13] I. N. Cangül, M. Demirci, G. Soydan and N. Tzanakis, The Diophantine equation $x^2 + 5^a \cdot 11^b = y^n$, Funct. Approx. Comment. Math., to appear, (arXiv:1001.2525).

[14] I. N. Cangül, M. Demirci, F. Luca, A. Pintér and G. Soydan, On the Diophantine equation $x^2 + 2^a \cdot 11^b = y^n$, Fibonacci Quart., to appear.

[15] I. N. Cangül, M. Demirci, I. Inam, F. Luca and G. Soydan, On the Diophantine equation $x^2 + 2^a \cdot 3^b \cdot 11^c = y^n$, submitted.

[16] E. L. Cohen, The Diophantine equation $x^2 + 11 = 3^k$ and related questions, Math. Scand. 38 (1976), 240-246.

[17] A. Dujella and A. Pethö, A generalization of a theorem of Baker and Davenport, Quart. J. Math. Oxford Ser. (2) 49 (1998), 291-306.

[18] C. Ko, On the Diophantine equation $x^2 = y^n + 1, xy \neq 0$, Sci. Sinica 14 (1965), 457-460.

[19] M. Le, An exponential Diophantine equation, Bull. Austral. Math. Soc. 64 (2001), 99-105.

[20] M. Le, On Cohn's conjecture concerning the Diophantine $x^2 + 2^m = y^n$, Arch. Math. (Basel) 78 (2002), 26-35.

[21] V. A. Lebesgue, Sur l'impossibilité en nombres entiers de l'equation $x^m = y^2 + 1$, Nouv. Annal. des Math. 9 (1850), 178-181.

[22] F. Luca, On a Diophantine equation, Bull. Austral. Math. Soc. 61 (2000), 241-246.

[23] F. Luca, On the Diophantine equation $x^2 + 2^a \cdot 3^b = y^n$, Int. J. Math. Math. Sci. 29 (2002), 239-244.

[24] F. Luca and A. Togbé, On the Diophantine equation $x^2 + 7^{2k} = y^n$, Fibonacci Quart. 54(4) (2007), 322-326.

[25] F. Luca and A. Togbé, On the Diophantine equation $x^2 + 2^a \cdot 5^b = y^n$, Int. J. Number Theory 4 (2008), 973-979.

[26] E. M. Matveev, An explict lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, II, Izv. Ross. Akad. Nauk Ser. Math. 64 (2000), 125-180, English transl. in Izv. Math. 64 (2000), 1217-1269.

[27] T. Nagell, Lϕsning til oppgave nr 2, 1943, s. 29, Nordisk Mat. Tidskr 30 (1948), 62-64.

[28] S. Ramanujan, Question 464, J. Indian Math. Soc. 5 (1913), 120.

[29] S. Ramanujan, Collected Papers, Chelsea Publishing Co., New York, (1962), 327.

[30] T. N. Shorey, Diophantine approximations, Diophantine equations, transcendence and applications, Indian J. Pure Appl. Math. 37 (2006), 9-39.

[31] Sz. Tengely, On the Diophantine equation $x^2 + a^2 = 2y^p$, Indag. Math. (N.S.) 15 (2004), 291-304.

■