Acta Math. Univ. Comenianae
Vol. LXXXVII, 2 (2018), pp. 199–204

THE DIOPHANTINE EQUATIONS $2^n \pm 3 \cdot 2^m + 9 = x^2$

K. GUETH AND L. SZALAY

ABSTRACT. In this paper, we study the diophantine equations, $2^n \pm 3 \cdot 2^m + 9 = x^2$, and apart from the plus case with the condition, $n < m$ we solve completely the problem. The method resembles the treatment was used, to solve the equation $2^n + 2^m + 1 = x^2$. The more general problem $2^n \pm \alpha \cdot 2^m + \alpha^2 = x^2$, where α is an odd prime such that 2 is a non-quadratic residue modulo α is also considered.

1. INTRODUCTION

There are several works on determining full squares in specified infinite sets of integers, and some of them claim a few nonzero digits in base p. For instance, the simple equation $2^n + 1 = x^2$ with positive integers n asks the odd integers x having two 1 bits in the binary expansion of its square. Szalay [**7**] studied the analogous equation with three 1 bits. He proved that the equation $2^n + 2^m + 1 = x^2$ with integers $n \geq m \geq 0$ and $x \geq 0$ has only the solutions $(n, m, x) = (2t, t + 1, 2^t + 1)$ with integer $t \geq 1$, and $(n, m, x) = (1, 0, 2)$, $(5, 4, 7)$, $(9, 4, 23)$. The proof of the theorems of this paper is built upon the method worked out in [**7**]. The equation $2^n - 2^m + 1 = x^2$ was also considered there. The solutions are $(n, m, x) = (2t, t + 1, 2^t - 1)$ $(t \geq 2)$, $(n, m, x) = (t, t, 1)$ $(t \geq 1)$, and $(n, m, x) = (5, 3, 5)$, $(7, 3, 11)$, $(15, 3, 181)$. Luca [**5**] extended the problem to arbitrary odd prime base p and proved that the equation $p^n + p^m + 1 = x^2$ possesses no integer solutions. Bennett and Bugeaud [**1**] showed that if $s^n + s^m + 1 = x^2$ holds for an odd integer s with $n > m > 0$, then $\min\{\gcd(s, x - 1), \gcd(s, x + 1)\} > x^{1/6}$ and the exponent $1/6$ can be replaced by an arbitrary real number less then $1/4$ if x is large enough.

The question arises naturally: what happens if the square is replaced by any pure power? The same paper of Bennett and Bugeaud [**1**] contains the following result. If $s^n + s^m + 1 = x^k$ holds for the positive integers s, $n > m$, $k \geq 2$ with $\gcd(k, \varphi(s)) = 1$, then $(s, n, m, x^k) = (2, 5, 4, 7^2)$, $(2, 9, 4, 23^2)$, $(3, 7, 2, 13^3)$, or $(2, 2t, t + 1, (2^t + 1)^2)$ $(t \geq 1)$. When we omit the condition $\gcd(k, \varphi(s)) = 1$, but we assume $s = 2$ or 3, then the equation has the same set of solutions (see [**2**] and [**1**]).

Received July 19, 2017; revised January 7, 2018.
2000 *Mathematics Subject Classification.* Primary 11D61.
Key words and phrases. diophantine equations; polynomial-exponential equations; number of bits in squares.

Another extension of the problem appears when one takes different bases of powers. In this direction, Hajdu and Pink [**3**] completely solved the diophantine equation $1+2^a+t^b=x^k$ assuming odd $t\leq 50$. Later Bérczes et al. [**4**] examined the more general equation $1+s^a+t^b=x^k$ and provided all the solutions with the conditions $k\geq 4$, $1\leq s,t\leq 50$, and $s\not\equiv t \pmod 2$.

Now we consider a new variation of the equations $2^n\pm 2^m+1=x^2$ as follows. By multiplying the second 2-power by 3, and replacing the constant 1 term by 9, we obtain the title equations. We will show that in the negative case, and in the positive case with $n\geq m$ there is an infinite family of solutions described by one parameter, respectively, and there exist a few sporadic solutions which do not belong to the aforementioned family. More precisely, we obtained the following two theorems.

Theorem 1. *If* $2^n-3\cdot 2^m+9=x^2$ *holds for some non-negative integers* n,m *and* x*, then*

- *either* $(n,m,x)=(2t,t+1,|2^t-3|)$, $t\in\mathbb{N}$,
- *or* $(n,m,x)=(6,3,7)$.

Theorem 2. *If* $2^n+3\cdot 2^m+9=x^2$ *holds for some non-negative integers* $n\geq m$ *and* x*, then*

- *either* $(n,m,x)=(2t,t+1,2^t+3)$, $1\leq t\in\mathbb{N}$,
- *or* $(n,m,x)=(2,0,4)$, $(6,5,13)$, $(8,3,17)$.

Based on a computer search, we conjecture that in the case $n<m$ there are only four solutions to $2^n+3\cdot 2^m+9=x^2$.

Conjecture 1. Assume that $2^n+3\cdot 2^m+9=x^2$ is fulfilled for some non-negative integers $n<m$ and x. Then

$$(n,m,x)=(0,1,4),\ (4,5,11),\ (6,8,29),\ (6,13,157).$$

Although elementary approach may also be possible, the proofs of the two theorems use willfully the method of [**7**] to demonstrate that it works for other problems. In the next section, we describe the auxiliary lemmata useful in the proofs.

2. Lemmata

Lemma 1. *Let* $0\neq D\in\mathbb{Z}$*. If* $|D|<2^{96}$ *and* $2^n+D=x^2$ *has a solution* (n,x)*, then*

$$n<18+2\log_2|D|.$$

Proof. This is [**6**, Corollary 2] due to Beukers. □

Lemma 2. *If* t*,* x *and* y *are positive integers satisfying*

$$y^2-9=2^{2t}\left(x^2-9\right),\qquad y\geq 4,\ x\geq 4, \tag{1}$$

then

- *either* $(x, y) = (3 \cdot 2^{t-1}, 3 \cdot (2^{2t-1} - 1))$ *with* $t \geq 2$,
- *or* $(t, x, y) = (1, 7, 13)$, $(2, 4, 11)$, $(2, 17, 67)$.

Proof. Observe that if t is fixed, then the equivalent form $9 \cdot (2^{2t} - 1) = (2^t x - y) \cdot (2^t x + y)$ of (1) can be easily solved. Accordingly, (1) has only the solution $(x, y) = (7, 13)$ if $t = 1$, further $(x, y) = (4, 11)$, $(17, 67)$, and $(6, 21)$ are deduced from $t = 2$. But the last pair is included in the infinite family $(x, y) = (3 \cdot 2^{t-1}, 3 \cdot (2^{2t-1} - 1))$. Suppose now that $t \geq 3$, $y \geq 4$, and $x \geq 4$ satisfy (1). Then y is necessarily odd and we have

$$\frac{y-3}{2} \cdot \frac{y+3}{2} = 2^{2t-2}\left(x^2 - 9\right). \tag{2}$$

The greatest common divisor of $(y-3)/2$ and $(y+3)/2$ is 1 or 3. Hence 2^{2t-2} divides exactly one of the terms on the left hand side of (2). Consequently, $y = 2^{2t-1}k \pm 3$ with some integer $k \geq 1$, moreover, it follows that

$$\frac{y^2 - 9}{2^{2t}} = 2^{2t-2}k^2 \pm 3k = x^2 - 9. \tag{3}$$

By (1), we even conclude

$$y < 2^t x. \tag{4}$$

Assume first that $y = 2^{2t-1}k + 3$. Then by (4), we obtain $2^{t-1}k + 1 \leq x$ and together with (3), the inequality $3k + 9 \geq 2^t k + 1$ follows. Thus

$$8 \geq (2^t - 3)k,$$

and we deduce $t = 3$ and $k = 1$. Subsequently, $y = 35$, and then $x^2 = 28$, a contradiction.

Now we suppose that $y = 2^{2t-1}k - 3$. Combining it with (4), it results $2^{t-1}k \leq x$. Then (3) provides $3 \geq k$. We distinguish three cases according to the value of k.

The case $k = 1$ leads to $2^{2t-2} + 6 = x^2$, and the factorization $6 = (x - 2^{t-1}) \cdot (x + 2^{t-1})$ shows no solution. Similarly, if $k = 2$, then $2^{2t} + 3 = x^2$, and there is no solution with $t \geq 3$. Finally, $k = 3$ returns with the infinite family

$$x = 3 \cdot 2^{t-1}, \; y = 3 \cdot \left(2^{2t-1} - 1\right),$$

where $t \geq 3$, and together with $(x, y) = (6, 21)$, we get the complete family. □

Remark 3. At the application of this lemma only those cases are important where x is odd, i.e., $(t, x, y) = (1, 7, 13)$, $(2, 17, 67)$.

3. Proof of the theorems

3.1. Proof of Theorem 1.

Proof. Considering the equation

$$2^n - 3 \cdot 2^m + 9 = x^2 \tag{5}$$

modulo 3, it follows that n is even. Obviously, each element of the set

$$F = \{(n, m) \in \mathbb{N}^2 \mid n = 2t, \, m = t + 1, \, t \in \mathbb{N}\}$$

with suitable $x \in \mathbb{N}$ satisfies (5). Let S denote the set of all solutions (n, m) to (5), further let $E = \{(6,3)\}$. We have to show that $S = F \cup E$.

The condition $n \leq m+1$ immediately leads to $0 \leq x^2 \leq 2^{m+1} - 3 \cdot 2^m + 9 = 9 - 2^m$. Thus $m \leq 3$, and we easily check the possible range. We obtain the solutions

$$(n, m, x) = (0,1,2),\ (2,2,1),\ (4,3,1),$$

but these are included in the infinite family F.

In the sequel, we may assume that $n \geq m+2$. First verify the cases $m \in \{0,1,2\}$. Lemma 1 provides the upper bound $n < 23.2$ if $m = 0$, and $n \leq 21.2$ if $m = 1$ or 2. Checking the possible ranges, we find no solution with $n \geq m+2$. We note that the same outcome can be obtained without the application of Beukers's lemma if one recalls that n is even, hence the corresponding integer equals the difference of two squares.

Suppose now that $m \geq 3$. Subsequently, $n \geq 5$. Clearly, x is odd, further $x \geq 5$. Observe that if $(n, m) \in S$, $n \geq m+2$ hold, then $2^{n-m} - 3 = (x^2 - 9)/2^m \in \mathbb{N}$, further

$$2^{2n-2m} - 3 \cdot 2^{n-m+1} + 9 = \left(\frac{x^2 - 9}{2^m}\right)^2.$$

Hence a solution (n, m) of (5) provides $(2n - 2m, n - m + 1) \in F \subset S$. Then the transformation

$$\tau\colon (n, m) \mapsto (2n - 2m, n - m + 1), \qquad n \geq m+2,$$

induces a map of $S \setminus \{(0,1),(2,2),(4,3)\}$ into $F \setminus \{(0,1),(2,2)\}$.

The map τ has a great importance with useful properties. If $(n, m) \in S$, then let $\delta(n, m) \in \mathbb{Z}$ denote the distance $n - m$ of the exponents n and m.

Property 1. $\delta(\tau(n,m)) = \delta(n,m) - 1$. In particular, $\tau(n,m) \neq (n,m)$, i.e., the map has no fixed points.

Property 2. If $(n,m) \in F \setminus \{(0,1),(2,2),(4,3)\}$, more precisely, if $(n,m) = (2t, t+1)$, $t \geq 3$, then $\tau(n,m) = (2t-2, t) \in F$ is the '*lower neighbor*' solution of (n,m) in F. Thus the elements of the set F are ordered by τ. Moreover $\delta(\tau(2t, t+1)) = t - 2$ shows by $t \geq 3$ that all positive integers occur as a difference of the exponents in the solution of (5).

Property 3. If (n,m) is an exceptional solution, i.e., $(n,m) \in S \setminus F$, then $\tau(n,m) \in F$ since $\tau(n,m) = (2\delta(n,m), \delta(n,m)+1)$. Especially, $\tau(6,3) = (6,4)$.

Note that $\tau(4,3) = (2,2)$ and $\tau(2,2) = (0,1)$ also hold.

By Properties 1–3, we have to prove that there is exactly one case when $(n,m) \neq (n_1, m_1)$ and $\tau(n,m) = \tau(n_1, m_1)$. In other words, we must show that the system of the equations

$$\begin{aligned} 2^n - 3 \cdot 2^m + 9 &= x^2 \\ 2^{n+d} - 3 \cdot 2^{m+d} + 9 &= y^2 \end{aligned} \tag{6}$$

in positive integers n, m, d, x, y with $3 \leq m$, $m+2 \leq n$ has exactly one solution with odd $x < y$.

These equalities imply

$$y^2 - 9 = 2^d \left(x^2 - 9\right). \tag{7}$$

Take (6) modulo 3. Thus d must be even since n is even. Put $d = 2t$ and apply Lemma 2. In the solutions provided by the lemma, the parity of x is even, except the cases when $(d, x, y) = (2, 7, 13)$, $(4, 17, 67)$. Hence we distinguish two cases.

First suppose $x = 17$. Then $2^n - 3 \cdot 2^m + 9 = 17^2$ does not hold. Indeed, $2^n - 3 \cdot 2^m = 17^2 - 9 = 2^3 \cdot 35$, so $m = 3$, and then $2^{n-m} - 3 = 35$ is a contradiction.

Hence only $(d, x, y) = (2, 7, 13)$ is possible, and it gives $n = 6$, $m = 3$ via $2^n - 3 \cdot 2^m + 9 = 7^2$ and $2^{n+2} - 3 \cdot 2^{m+2} + 9 = 13^2$. Observe that we have found the exceptional solution $(n, m, x) = (6, 3, 7)$ while the pair $(n+d, m+d, y) = (8, 5, 13)$ appears in F.

The proof of Theorem 1 is completed. □

3.2. Proof of Theorem 2.

Proof. Recall that along this subsection we always assume $n \geq m$. We follow the method we used during the previous proof. The machinery is the same, therefore, we are concentrating only on the deviation. We know that n must be even again, we have the infinite family

$$F = \{(n, m) \in \mathbb{N}^2 \mid n = 2t,\ m = t + 1,\ t \in \mathbb{N}^+\}$$

of solutions to $2^n + 3 \cdot 2^m + 9 = x^2$. We use Beukers's lemma (Lemma 1) to handle the cases $n = m$,, and $m = 0$, which provide only $(n, m, x) = (2, 0, 4)$ as exceptional solution (i.e., not in F). Here an elementary treatment would also be possible. When $n > m \geq 1$ then taking square of both sides of the equality $2^{n-m} + 3 = (x^2 - 9)/2^m$ leads to the transformation

$$\tau\colon (n, m) \mapsto (2n - 2m, n - m + 1).$$

Map τ has again the same three properties, and now we must study the system

$$\begin{aligned} 2^n + 3 \cdot 2^m + 9 &= x^2 \\ 2^{n+d} + 3 \cdot 2^{m+d} + 9 &= y^2 \end{aligned} \tag{8}$$

in positive integers n, m, d, x, y with $m + 1 \leq n$, $x \equiv y \equiv 1 \pmod 2$. The system above implies again (7)

$$y^2 - 9 = 2^d \left(x^2 - 9\right).$$

A modulo 3 consideration of (8) shows that d is also even.

Lemma 2 admits only $(d, x, y) = (2, 7, 13)$, $(4, 17, 67)$ because x is odd. Both are possible since

$$2^n + 3 \cdot 2^m + 9 = 7^2 \qquad \text{and} \qquad 2^{n+2} + 3 \cdot 2^{m+2} + 9 = 13^2,$$

further

$$2^n + 3 \cdot 2^m + 9 = 17^2 \qquad \text{and} \qquad 2^{n+4} + 3 \cdot 2^{m+4} + 9 = 67^2$$

are solvable by $(n, m) = (4, 3)$, and $(n, m) = (8, 3)$, respectively. Thus we have found the two exceptional solutions $(n, m, x) = (6, 5, 13)$ and $(8, 3, 17)$.

The proof of Theorem 2 is completed. □

4. General remarks

The methods we used in the proof of Lemma 2 and in the proofs of the theorems can be applied for other equations. Assume that α is a fixed odd prime such that 2 is a quadratic non-residual modulo α. Then the equations

$$2^n \pm \alpha \cdot 2^m + \alpha^2 = x^2$$

can be handled by a similar way ($n \geq m$ is supposed at $2^n + \alpha \cdot 2^m + \alpha^2 = x^2$).

Indeed, the non-quadratic residual condition guarantees that n is even. Clearly, it plays a crucial role to reduce to even d in the analogous equation of (6) or (8) (and then (7)). The transformation τ exists analogously with the same properties. Finally, the solution of the equation

$$y^2 - \alpha^2 = 2^{2t}(x^2 - \alpha^2)$$

corresponding to Lemma 2 can be treated by the same machinery.

References

1. Bennett M. and Bugeaud Y., *Perfect powers with three digits*, Mathematika, **60** (2014), 66–84.
2. Bennett M., Bugeaud Y. and Mignotte M., *Perfect powers with few binary digits and related Diophantine problems II.*, Math. Proc. Cambridge Philos. Soc. **153** (2012), 525–540.
3. Hajdu L., Pink I., On the Diophantine equation $1 + 2^a + x^b = y^n$, J. Number Theory **143** (2014), 1–13.
4. Bérczes A., Hajdu L., Miyazaki T. and Pink I., *On the Diophantine equation* $1+x^a+z^b = y^n$, J. Comb. Number Theory **8** (2016), 145–154.
5. Luca F., *The Diophantine equation* $x^2 = p^a \pm p^b + 1$, Acta Arithm. **112** (2004), 87–101.
6. Beukers F., *On the generalized Ramanujan-Nagell equation I.*, Acta Arithm. **83** (1981), 389–410.
7. Szalay L., *The equations* $2^N \pm 2^M \pm 2^L = z^2$, Indag. Math. (N. S.), **13** (2002), 131–142.

K. Gueth, Eötvös Loránd University, 9700 Szombathely, Károli G. tér 4, Hungary,
e-mail: `guethk@gmail.com`

L. Szalay, Institute of Mathematics, Faculty of Forestry, University of West Hungary, H-9400 Sopron, Hungary and J. Selye University, Komárno, Bratislavská cesta 3322, Slovakia,
e-mail: `laszlo.szalay.sopron@gmail.com`