On the Diophantine equations $(2^n-1)(6^n-1)=x^2$ and $(a^n-1)\left(a^{kn}-1\right)=x^2$

Lajos Hajdu[1] and László Szalay[2]

Abstract

In this paper we prove that the equation $(2^n-1)(6^n-1)=x^2$ has no solutions in positive integers n and x. Furthermore, the equation $(a^n-1)\left(a^{kn}-1\right)=x^2$ in positive integers $a>1$, n, $k>1$ ($kn>2$) and x is also considered. We show that this equation has the only solutions $(a,n,k,x)=(2,3,2,21)$, $(3,1,5,22)$ and $(7,1,4,120)$.

1 Introduction

In the present paper we prove two results.

Theorem 1. *The equation*

$$(2^n-1)(6^n-1)=x^2 \tag{1}$$

has no solutions in positive integers n and x.

---

[0] *Mathematics subject classification numbers,* 11B37, 11D61.

Key words and phrases. Linear recurrence, pure powers.

[1] Research supported in part by the Hungarian Academy of Sciences, by the János Bolyai Research Fellowship and by Grants T29330 and 023800 of the Hungarian National Foundation for Scientific Research.

[2] Research supported by Hungarian National Foundation for Scientific Research Grant No. 25157/1998.

Theorem 2. *The equation*

$$(a^n - 1)\left(a^{kn} - 1\right) = x^2 \tag{2}$$

has the only solutions $(a, n, k, x) = (2, 3, 2, 21)$, $(3, 1, 5, 22)$ *and* $(7, 1, 4, 120)$ *in positive integers* $a > 1$, n, $k > 1$ $(kn > 2)$ *and* x.

The left hand sides of these equations satisfy a fourth order linear recursive relations. Thus the solution of these mixed exponential-polynomial diophantine equations is equivalent to the determination of all perfect squares in fourth order recurrences.

In case of fourth order recurrences there are results which are similar to Theorem 1 only for some classes of Lehmer sequences of first and second kind. These were obtained by McDaniel, who examined the existence of perfect square terms of Lehmer sequences in [3].

The second author of this paper has shown (see [4]) that the equation $(2^n - 1)(3^n - 1) = x^2$ has no positive integer solutions, and the equation $(2^n - 1)(5^n - 1) = x^2$ has the only solution $n = 1$, $x = 2$ in positive integers n and x. In [4] the second title equation has also been examined in the special case $a = 2$. Thus our Theorem 2 generalizes that result.

Let p be a rational prime number and n be an integer. In the sequel $\left(\frac{n}{p}\right)$ denote the Legendre symbol with respect to these numbers.

2 Preliminaries

We need the following theorems in the proof of Theorem 2.

Theorem A. (Ljunggren, [2]) *The diophantine equation*

$$\frac{x^n - 1}{x - 1} = y^2 \quad , \quad (n > 2)$$

is impossible in integers x, y $(|x| > 1)$, *except when* $n = 4$, $x = 7$ *and* $n = 5$, $x = 3$.

Theorem B. (Chao Ko, [1]) *The equation*

$$x^p + 1 = y^2 \quad ,$$

where p is a prime greater than 3, has no solution in integers $x \neq 0$ and y.

3 Proof of the Theorems

3.1 Proof of Theorem 1

Suppose that (n, x) is a solution of equation (1). If n is odd then $(2^n - 1)(6^n - 1) \equiv -1 \pmod 3$ which cannot be a square. Now we can assume that n is even and distinguish two cases.

I. First put $n = 4t$ with some positive integer t, and write $t = k \cdot 5^{\alpha-1}$, where k and α are positive integers with $5 \nmid k$.

Then we have $(2^n - 1)(6^n - 1) = \left(16^{k5^\alpha} - 1\right)\left(1296^{k5^\alpha} - 1\right)$. Since $1296 \equiv 1 - 5 \pmod{5^2}$ it follows that $1296^5 \equiv 1 - 5^2 \pmod{5^3}$ and inductively $1296^{5^{\alpha-1}} \equiv 1 - 5^\alpha \pmod{5^{\alpha+1}}$. Thus $1296^t \equiv 1 - k \cdot 5^\alpha \pmod{5^{\alpha+1}}$. Similarly (or by [4]), $16^t \equiv 1 + 3k \cdot 5^\alpha \pmod{5^{\alpha+1}}$. Consequently $\frac{2^n-1}{5^\alpha} \equiv 3k \pmod 5$ and $\frac{6^n-1}{5^\alpha} \equiv -k \pmod 5$, and we can re-write equation (1) as

$$\frac{2^n - 1}{5^\alpha} \frac{6^n - 1}{5^\alpha} = x_1^2 \quad , \tag{3}$$

where $x_1 = \frac{x}{5^\alpha}$ and the prime 5 divides neither the left nor the right hand side of (3). However, for the Legendre symbol of the left hand side of (3) we obtain

$$\left(\frac{\frac{2^n-1}{5^\alpha} \frac{6^n-1}{5^\alpha}}{5}\right) = \left(\frac{3k}{5}\right)\left(\frac{-k}{5}\right) = \left(\frac{-3}{5}\right) = -1 \quad ,$$

which is a contradiction. Thus Theorem 1 is proved in case I.

II. Now let $n = 4t + 2 = 2(2t + 1)$, where t is a natural number. In this case we must investigate the equation $(4^u - 1)(36^u - 1) = x^2$ for odd $u = 2t + 1$. This last equation is also satisfied $\pmod{18}$, hence it is easy to verify that 3 must divide u. Then we have to solve the equation

$$(64^w - 1)\,(46656^w - 1) = x^2$$

in odd positive integers $w = \frac{u}{3}$. To show the insolvability of this equation, we give two positive integers such that no term of the sequence $(64^w - 1)(46656^w - 1)$ is a quadratic residue for both the given two numbers as moduli. For example, 17 and 97 are such numbers.

To prove this, let $I_w = (64^w - 1)(46656^w - 1)$. Then

$$I_w \equiv ((-4)^w - 1)(8^w - 1) \pmod{17} \quad .$$

Since

$$(-4)^4 \equiv 1 \pmod{17} \text{ and } 8^8 \equiv 1 \pmod{17} \quad ,$$

it is sufficient to examine the cases $w = 1, 3, 5, 7$.

$$I_1 \equiv 16 \pmod{17} \text{ and } I_7 \equiv 8 \pmod{17}$$

are quadratic residues, while

$$I_3 \equiv 3 \pmod{17} \text{ and } I_5 \equiv 11 \pmod{17}$$

are not quadratic residues $\pmod{17}$.

On the other hand,

$$I_w \equiv (64^w - 1)((-1)^w - 1) \equiv (64^w - 1)(-2) \pmod{97} \quad .$$

Since $64^8 \equiv 1 \pmod{97}$, we must investigate the cases $w = 1, 3, 5, 7$.

$$I_1 \equiv 68 \pmod{97} \text{ and } I_7 \equiv 5 \pmod{97}$$

are not quadratic residues, but

$$I_3 \equiv 96 \pmod{97} \text{ and } I_5 \equiv 33 \pmod{97}$$

are quadratic residues $\pmod{97}$. This completes the proof of the Theorem. ■

3.2 Proof of Theorem 2

Suppose that the four-tuple (a, n, k, x) $(a > 1, k > 1, kn > 2)$ is a solution of equation (2). Let $y = a^n$. Now we have the equality

$$x^2 = (y-1)^2(y^{k-1} + \ldots + y + 1) = (y-1)^2 \left(\frac{y^k - 1}{y-1}\right) \quad .$$

Thus $\frac{y^k-1}{y-1}$ must be a square. By Theorem A, if $k > 2$ then $k = 4$ or $k = 5$. Consequently from $y = a^n = 7$ it follows that $a = 7, n = 1, x = 120$ and $y = a^n = 3$ gives $a = 3, n = 1, x = 22$. These two cases provide the solutions $(a, k, n, x) = (7, 4, 1, 120)$ and $(3, 5, 1, 22)$ of (2).

Now suppose that $k = 2$. Then $(y-1)^2(y+1) = x^2$ and

$$y + 1 = a^n + 1 \tag{4}$$

must be a square. Since $kn > 2$, it follows that $n > 1$. Without loss of generality we may assume that n is a prime. If $n = 2$ then (4) cannot be a square, and it is well known that if $n = 3$ then for a positive integer a, (4) is a square only in case of $a = 2$. Thus equation (2) has one more solution: $(a, k, n, x) = (2, 2, 3, 21)$. Finally, by Theorem B (4) cannot be a square if $n > 3$. This completes the proof of Theorem 2. $\blacksquare$

Remark. If $k = 1$ then $(a^n - 1)(a^n - 1)$ is always square number. If $k = 2$ and $n = 1$ then $(a-1)(a^2-1) = (a-1)^2(a+1)$ may be square infinitely many times when $a + 1$ is a square.

Acknowledgements. The authors are grateful to the referee for his many useful remarks and suggestions.

References

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

[2] Ljunggren, W., Some theorems on indeterminate equations of the form $(x^n - 1)/(x - 1) = y^q$ (Norvegian), Norsk Mat. Tidsskr. **25** (1943), 17-20.

[3] McDaniel W. L., Square Lehmer numbers, Colloq. Math. **66** (1993), 85-93.

[4] Szalay, L., On the diophantine equation $(2^n-1)(3^n-1)=x^2$, Publ. Math. Debrecen **57** (2000), 1-9.

Lajos Hajdu
University of Debrecen
Institute of Mathematics and Informatics
Debrecen, P.O.Box 12.
H-4010, Hungary
e-mail: hajdul@math.klte.hu

László Szalay
University of West Hungary
Institute of Mathematics
Sopron, Bajcsy Zs. u. 4.
H-9400, Hungary
e-mail: laszalay@efe.hu