Publ. Math. Debrecen
57 / 1-2 (2000), 1–9

On the diophantine equation $(2^n-1)(3^n-1)=x^2$

By LÁSZLÓ SZALAY (Sopron)

Abstract. This paper determines all the solutions of the diophantine equations $(2^n-1)(3^n-1)=x^2$, $(2^n-1)(5^n-1)=x^2$ and $(2^n-1)((2^k)^n-1)=x^2$ in positive integers n and x. The proofs depend on the theory of quadratic residuals in the case of the first two equations. For the third one we use a famous result of Ljunggren.

1. Introduction

In this paper we will study the title equation

$$(2^n-1)\,(3^n-1)=x^2 \tag{1}$$

in positive integers n and x. We will prove that it has no solution, and using the same method, the equation

$$(2^n-1)\,(5^n-1)=x^2 \tag{2}$$

will also be investigated. This equation has only one solution: $n=1$, $x=2$. We will also consider the equation

$$(2^n-1)\left(\left(2^k\right)^n-1\right)=x^2 \tag{3}$$

with $k>1$ ($k\in\mathbb{Z}$).

Mathematics Subject Classification: 11B, 11D.
Key words and phrases: recurrence sequences, polynomial-exponential diophantine equations.
Research supported by Hungarian National Foundation for Scientific Research Grant No. 25157/1998.

Let A_1, A_2, R_0, R_1 be integers and $R = R(A_1, A_2, R_0, R_1)$ be a second order linear recurrence defined by

$$R_n = A_1 R_{n-1} + A_2 R_{n-2} \quad (n \geq 2). \tag{4}$$

With integer initial values G_0, G_1, G_2, G_3 and integer coefficients A_1, A_2, A_3, A_4, we also define a fourth order linear recursive sequence G by

$$G_n = A_1 G_{n-1} + A_2 G_{n-2} + A_3 G_{n-3} + A_4 G_{n-4} \quad (n \geq 4). \tag{5}$$

Let the recurrence (5) be denoted by $G(A_1, A_2, A_3, A_4, G_0, G_1, G_2, G_3)$. The terms $2^n - 1$, $3^n - 1$, $5^n - 1$ and $(2^k)^n - 1$ satisfy the binary recurrence relations $R^{(2)}(3, -2, 0, 1)$, $R^{(3)}(4, -3, 0, 2)$, $R^{(5)}(6, -5, 0, 4)$ and $R^{(2^k)}(2^k + 1, -2^k, 0, 2^k - 1)$, respectively. The products $(2^n - 1)\,(3^n - 1)$, $(2^n - 1)(5^n - 1)$ and $(2^n - 1)((2^k)^n - 1)$ also satisfy the fourth order linear recursive relations $G^{(3)}(12, -47, 72, -36, 0, 2, 24, 182)$, $G^{(5)}(18, -97, 180, -100, 0, 4, 72, 868)$ and $G^{(2^k)}(3(2^k + 1), -(2^{2k+1} + 9 \cdot 2^k + 2), 6 \cdot 2^k(2^k + 1), 2^{2k+2}, 0, 2^k - 1, 3 \cdot (2^{2k} - 1), 7 \cdot (2^{3k} - 1))$, respectively. Thus, to solve the mixed exponential-polynomial diophantine equation (1) (or (2) or (3)) is equivalent to the determination of all perfect squares in a fourth order recurrence or in the products of the terms of two binary sequences. This new interpretation provides the equations

$$G_n^{(3)} = x^2 \quad \text{or} \quad R_n^{(2)} \cdot R_n^{(3)} = x^2, \tag{6}$$

$$G_n^{(5)} = x^2 \quad \text{or} \quad R_n^{(2)} \cdot R_n^{(5)} = x^2, \tag{7}$$

and with $k > 1$

$$G_n^{(2^k)} = x^2 \quad \text{or} \quad R_n^{(2)} \cdot R_n^{(2^k)} = x^2. \tag{8}$$

In case of the fourth order recurrences similar results are known only for some classes of Lehmer sequences of first an second kind. In [6] McDaniel examined the existence of perfect square terms of Lehmer sequences and gained interesting theorems.

Many authors investigated the squares and pure powers in binary recurrences. Cohn [1] and Wyler [13], applying elementary methods, proved independently that the only square in Fibonacci numbers are $F_0 = 0$, $F_1 = F_2 = 1$ and $F_{12} = 144$. For Lucas numbers Cohn [2] showed that if $L_n = x^2$ then $n = 1$, $x = 1$ or $n = 3$, $x = 2$. Pethő [7] gave all pure powers in the Pell sequence. In [10], under some conditions, Ribenboim and McDaniel showed that the square classes of the Lucas sequence $U(P, Q, 0, 1)$ contain at most 3 elements, except one case. Analogous results are established for the associate sequence V of U. In [11] the same authors determined – under some conditions – all squares in the sequences U and V.

There are more general results concerning pure powers in linear recurrences. Shorey and Stewart [12] proved that the terms of a nondegenerate recurrence sequence cannot be q-th powers for q sufficiently large if the characteristic polynomial of the sequence has a unique zero of largest absolute value. They, as well as Pethő [8], [9], gained a similar theorem for binary recurrences. Unfortunately, this general result gives no information about the low exponents, for example squares belonging to linear recurrences.

In the sequel we denote by $\nu_p(k)$ the p-adic value of the integer k, where p is a fixed rational prime number. As usual, $\phi(k)$ denotes the Euler function, $d(k)$ denotes the number of divisors function, and $\sigma(k)$ the sum of divisors function.

2. Theorems

The following theorems formulate precisely the statements mentioned in the introduction. Some corollaries of the results are also described here.

Theorem 1. *The equation*

$$(2^n - 1)(3^n - 1) = x^2 \tag{9}$$

has no solutions in positive integers n and x.

Theorem 2. *The equation*

$$(2^n - 1)(5^n - 1) = x^2 \tag{10}$$

has the only solution $n = 1$, $x = 2$ in positive integers n and x.

Theorem 3. *The equation*

$$(2^n - 1)\left((2^k)^n - 1\right) = x^2 \tag{11}$$

has the only solution $k = 2$, $n = 3$, $x = 21$ in positive integers $k > 1$, n and x.

We have the following immediate consequences of Theorems 1 and 2.

Corollary A. *The equation* $2 \cdot \sigma(6^n) = x^2$ *has no solution, the equation* $\sigma(10^n) = x^2$ *has the only solution* $n = 0$, $x = 1$.

Proof of Corollary A. We need to use the well-known result on the summatory function: $\sigma(k) = \prod_{p_i \mid k} \frac{p_i^{e_i+1}-1}{p_i-1}$, where $\nu_{p_i}(k) = e_i > 0$. $\square$

Corollary B. *The equation* $\sum_{i,j=1}^{n} \phi\left(2^i \cdot 3^j\right) = x^2$ *has no solution, the equation* $\sum_{i,j=1}^{n} \phi\left(2^i \cdot 5^j\right) = x^2$ *has only the solution* $n = 1$, $x = 2$.

Proof of Corollary B. These results follow from the multiplicativity of Euler's ϕ function and from the equality $p^n - 1 = \phi(p^n) + \phi(p^{n-1}) + \cdots + \phi(p)$, where p is a prime number. $\square$

It is interesting to observe that if one replaces Euler's ϕ function by the number of divisors function then for any primes p and q the sum

$$\sum_{i,j=1}^{n} d\left(p^i \cdot q^j\right) = \sum_{i,j=1}^{n} (i+1)(j+1) = \left(\sum_{k=2}^{n+1} k\right)^2 = \left(\frac{n(n+3)}{2}\right)^2 \tag{12}$$

is always a perfect square.

3. Preliminary lemmas

In our work we shall require Lemma 1, which we state without proof. (For a proof see e.g. [3], page 39.) Let $t > 1$ be an arbitrary integer and denote by $(\mathbb{Z}/t\mathbb{Z})^\star$ the multiplicative group of reduced residue classes modulo t.

Lemma 1. *Let* $\alpha > 1$ *be a rational integer and* p *an odd prime number. If* g *is a primitive root of* $(\mathbb{Z}/p\mathbb{Z})^\star$ *then*

a) g *is a primitive root of* $(\mathbb{Z}/p^\alpha\mathbb{Z})^\star$ *if* $g^{p-1} \not\equiv 1 \pmod{p^2}$, *and*

b) $g(p+1)$ *is a primitive root of* $(\mathbb{Z}/p^\alpha\mathbb{Z})^\star$ *if* $g^{p-1} \equiv 1 \pmod{p^2}$.

Lemma 1 immediately implies the following results by the choice of

a) $p = 3$, $g = 2$ and $g = 5$;

b) $p = 5$, $g = 2$ and $g = 3$.

Corollary of Lemma 1. *If* $\alpha > 1$ *is a rational integer then*

a) *the numbers 2 and 5 are primitive roots of* $(\mathbb{Z}/3^\alpha\mathbb{Z})^\star$, *and*

b) *the numbers 2 and 3 are primitive roots of* $(\mathbb{Z}/5^\alpha\mathbb{Z})^\star$.

Lemma 2. *Let α and k be positive integers with $k \not\equiv 0 \pmod 5$. If $n = k \cdot 4 \cdot 5^{\alpha-1}$ then*

$$\nu_5\left((2^n-1)(3^n-1)\right) = 2\alpha. \tag{13}$$

Proof of Lemma 2. Let us consider the congruences

$$2^n \equiv 1 \pmod{5^\alpha} \quad \text{and} \quad 3^n \equiv 1 \pmod{5^\alpha}, \tag{14}$$

where α is a fixed positive integer and n is unknown. According to the Corollary of Lemma 1b) and $\phi(5^\alpha) = 4 \cdot 5^{\alpha-1}$ we obtain the solutions $n = k \cdot 4 \cdot 5^{\alpha-1}$ $(k = 1, 2, \dots)$ for both congruences. If $k \not\equiv 0 \pmod 5$ then

$$2^n \not\equiv 1 \pmod{5^{\alpha+1}} \quad \text{and} \quad 3^n \not\equiv 1 \pmod{5^{\alpha+1}}. \tag{15}$$

So $\nu_5(2^n-1) = \alpha = \nu_5(3^n-1)$, which proves Lemma 2. □

Lemma 3. *Let α and k be positive integers with $k \not\equiv 0 \pmod 3$. If $n = k \cdot 2 \cdot 3^{\alpha-1}$ then*

$$\nu_3\left((2^n-1)(5^n-1)\right) = 2\alpha. \tag{16}$$

The proof of Lemma 3 is very similar to the previous one.

4. Proof of the theorems

4.1 Proof of Theorem 1

Suppose that the pair (n, x) is a solution of equation (9). Since $2 \mid (3^n-1)$ but $2 \nmid (2^n-1)$ for every positive integer n, it follows that $2 \mid x$, $4 \mid x^2$ and $4 \mid (3^n-1)$. Consequently n is an even number, but in this case $8 \mid (3^n-1)$ so $4 \mid x$, $16 \mid x^2$ and $16 \mid (3^n-1)$. From the last relation, in case n is even, it follows that n is divisible by 4 and can uniqely be written in the form $n = k \cdot 4 \cdot 5^{\alpha-1}$, where $1 \le \alpha \in \mathbb{Z}$ and $k \in \mathbb{Z}$, $k \not\equiv 0 \pmod 5$. Then, applying Lemma 2, we transform (9) into the form

$$\frac{2^n-1}{5^\alpha}\,\frac{3^n-1}{5^\alpha} = x_1^2, \tag{17}$$

where $x_1 = \frac{x}{5^\alpha}$ and the prime 5 divides neither the left nor the right hand side of (17). The Legendre symbol $\left(\frac{x_1^2}{5}\right) = 1$ because of $\gcd(x_1, 5) = 1$. On the other hand

$$\left(\frac{\frac{2^n-1}{5^\alpha}\,\frac{3^n-1}{5^\alpha}}{5}\right) = A \cdot B, \tag{18}$$

introducing the notation A and B for the Legendre symbols $\left(\frac{(2^n-1)/5^\alpha}{5}\right)$ and $\left(\frac{(3^n-1)/5^\alpha}{5}\right)$, respectively. We shall show that the calculation of A and B leads to a contradiction because the left side of (17) is not a quadratic residue modulo 5. More exactly, we shall prove that $A = \left(\frac{3k}{5}\right)$, $B = \left(\frac{k}{5}\right)$, so $AB = \left(\frac{3}{5}\right) = -1$. This means that the equation $(2^n-1)(3^n-1) = x^2$ has no solution in positive integers n and x. Now turn to the calculation of A and B.

Let $R = \alpha - 1$ and first let $k = 1$ (i.e. $n = 4 \cdot 5^R$). We are going to compute the residue of the expressions $\frac{2^{4\cdot 5^R}-1}{5^{R+1}}$ and $\frac{3^{4\cdot 5^R}-1}{5^{R+1}}$ after dividing them by 5.

a) If $R = 0$ then $\frac{2^4-1}{5} = 3 \equiv 3 \pmod 5$, and $\frac{3^4-1}{5} = 16 \equiv 1 \pmod 5$.

b) If $R = 1$ then

$$\frac{2^{4\cdot 5}-1}{5^2} = \frac{(2^4-1)}{5}\frac{\left(1+2^4+\cdots+\left(2^4\right)^4\right)}{5} = \frac{(2^4-1)}{5}\frac{Q_1}{5} \tag{19}$$

and

$$\frac{3^{4\cdot 5}-1}{5^2} = \frac{(3^4-1)}{5}\frac{\left(1+3^4+\cdots+\left(3^4\right)^4\right)}{5} = \frac{(3^4-1)}{5}\frac{Q_2}{5}. \tag{20}$$

Since $Q_1 \equiv Q_2 \equiv 5 \pmod{5^2}$ therefore $\frac{Q_1}{5} \equiv \frac{Q_2}{5} \equiv 1 \pmod 5$ and $\frac{2^{4\cdot 5}-1}{5^2} \equiv 3 \cdot 1 = 3 \pmod 5$, $\frac{3^{4\cdot 5}-1}{5^2} \equiv 1 \cdot 1 = 1 \pmod 5$.

c) If $R > 1$ then replace 2^4 by y in the first case and replace 3^4 by y in the second case. Thus for both cases

$$\frac{y^{5^R}-1}{5^{R+1}} = \tag{21}$$

$$= \frac{(y-1)(1+y+\ldots+y^4)(1+y^5+\ldots+y^{4\cdot 5})\cdots(1+y^{5^{R-1}}+\ldots+y^{4\cdot 5^{R-1}})}{5^{R+1}}.$$

Observe that $y^5 \equiv 1 \pmod{5^2}$, so each factor of the numerator is divisible by 5, but none of them is divisible by 5^2, consequently $\frac{y^{5^R}-1}{5^{R+1}} \equiv m \cdot 1 \cdots 1 \pmod{5}$, where $m=3$ if $y=2^4$ and $m=1$ if $y=3^4$.

These results make it possible to calculate the general case, when k is an arbitrary positive integer. Since $\frac{y^{5^R}-1}{5^{R+1}} \equiv m \pmod{5}$, therefore

$$y^{5^R} \equiv 1 + m \cdot 5^{R+1} \pmod{5^{R+2}}, \tag{22}$$

so

$$\left(y^{5^R}\right)^k \equiv \left(1 + m \cdot 5^{R+1}\right)^k \equiv 1 + k \cdot m \cdot 5^{R+1} \pmod{5^{R+2}}, \tag{23}$$

which means that

$$\frac{y^{k \cdot 5^R}-1}{5^{R+1}} \equiv k \cdot m \pmod{5}. \tag{24}$$

Our result concerning A and B follows from the last congruence. □

4.2 Proof of Theorem 2

Suppose that (n,x) is a solution of equation (10).

a) First we assume that n is even. Then n can uniquely be written in the form $n = k \cdot 2 \cdot 3^{\alpha-1}$, where $1 \leq \alpha \in \mathbb{Z}$ and $k \in \mathbb{Z}$, $k \not\equiv 0 \pmod{3}$. According to Lemma 3 we may transform (10) into the form

$$\frac{2^n-1}{3^\alpha} \, \frac{5^n-1}{3^\alpha} = x_1^2, \tag{25}$$

where $x_1 = \frac{x}{3^\alpha}$ and $\gcd(x_1,3)=1$, $\gcd(\frac{2^n-1}{3^\alpha},3)=1$ and $\gcd(\frac{5^n-1}{3^\alpha},3)=1$. To finish the proof of case a) we have to use step by step the same method as above, in the proof of Theorem 1. We will show the insolubility of equation (10) by evaluating the Legendre symbols of both sides of (10).

b) Let us continue the proof of Theorem 2 with the second case, when n is an odd integer.

If $n \equiv 3 \pmod{4}$ then we may write

$$\left(2^{4k+3}-1\right)\left(5^{4k+3}-1\right) = x^2, \quad (k \geq 0) \tag{26}$$

and it is easy to see that $2^{4k+3}-1 \equiv 7 \pmod{10}$ and $5^{4k+3}-1 \equiv 4 \pmod{10}$, from which it follows, in our case, that the left side of (26) is not a quadratic residue modulo 10.

Only the case $n \equiv 1 \pmod 4$ remains. If $2 \le n$ then equation (10) is equivalent to the equation

$$(2^n-1)(5^{n-1}+\cdots+5+1)=x_1^2, \tag{27}$$

where $x_1=\frac{x}{2}$. The corresponding congruence modulo 4 is

$$x_1^2 \equiv 3(1+\cdots+1)=3n \equiv 3 \pmod 4. \tag{28}$$

This is impossible, so we must finally check the case $n=1$. It provides the only solution of equation (10) since $(2^1-1)(5^1-1)=2^2$, and this is the assertion of Theorem 2. □

4.3 Proof of Theorem 3

Suppose that the triple (k,n,x) is a solution of equation (11), and let $y=2^n$. We have the equality

$$x^2=(y-1)^2(y^{k-1}+\cdots+y+1)=(y-1)^2\left(\frac{y^k-1}{y-1}\right). \tag{29}$$

Thus $\frac{y^k-1}{y-1}$ must be a square. In [5] Ljunggren proved that

$$\frac{y^k-1}{y-1}=x_1^2, \quad (k>2) \tag{30}$$

is impossible in integers $y>1$ and x_1, except when $k=4$, $y=7$, $x_1=20$ and $k=5$, $y=3$, $x_1=11$. But neither $y=7$ nor $y=3$ is a power of 2, so the equation (11) is not soluble if $k>2$. However, for $k=2$ only $n=3$ and $x=21$ satisfy the equation

$$(2^n-1)^2(2^n+1)=x^2 \tag{31}$$

since 2^n+1 is a perfect square if and only if $n=3$ (see e.g. [4]). This completes the proof of Theorem 3. □

References

[1] J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537–540.

[2] J. H. E. Cohn, Lucas and Fibonacci numbers and some diophantine equations, *Proc. Glasgow Math. Assoc.* **7** (1965), 24–28.

[3] N. Koblitz, A course in number theory and cryptography, *Springer-Verlag*, 1987.

[4] V. A. Lebesque, Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2+1$, *Nouv. Ann. Math.* **9** (1850), 178–81.

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

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

[7] A. Pethő, The Pell sequence contains only trivial perfect powers, Colloq. Math. Soc. János Bolyai 60, Sets, Graphs and Numbers Budapest (Hungary), 1991, 561–568.

[8] A. Pethő, Perfect powers in second order linear recurrences, *J. Num Theory* **15** (1982), 5–13.

[9] A. Pethő, Perfect powers in second order recurrences, Colloq. Math. Soc. János Bolyai 34, Topics in Classical Number Theory Budapest (Hungary), 1981, 1217–1227.

[10] P. Ribenboim and W. L. McDaniel, The square classes in Lucas sequences with odd parameters, *C. R. Math. Acad. Sci., Soc. R. Can.* **18** (1996), 223–227.

[11] P. Ribenboim and W. L. McDaniel, The square terms in Lucas sequences, *J. Number Theory* **58** (1996), 204–123.

[12] T. N. Shorey and C. L. Stewart, On the diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences, *Math. Scand.* **52** (1983), 24–36.

[13] O. Wyler, In the Fibonacci series $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ the first, second and twelfth terms are squares, *Amer. Math. Monthly* **71** (1964), 220–222.

LÁSZLÓ SZALAY
INSTITUTE OF MATHEMATICS
UNIVERSITY OF SOPRON
H–9400 SOPRON, BAJCSY ZS. U. 4.
HUNGARY

E-mail: laszalay@efe.hu

(Received December 18, 1998; revised May 3, 1999)