

The Pell Sequence Contains Only Trivial Perfect Powers

A. PETHŐ*

1. Introduction

Let $A, B \in \mathbb{Z}$, $|B| = 1$, $R_0 = 0$, $R_1 = 1$ and

$$R_{n+2} = AR_{n+1} - BR_n \quad (1)$$

for $n \geq 0$. We consider the equation

$$R_n = x^q \quad (2)$$

in integers n, x, q subject to $|x| > 1$, $q \geq 2$.

Shorey and Stewart [8] and independently Pethő [4] proved that (2) has only finitely many effectively computable solutions in n, x, q . Using only this result it is hopeless to solve completely (2) for given A and B because the bound for q is very large. It is about 10^{60} even in the modest cases. Equation (2) was examined by several authors for the Fibonacci sequence, which is defined by $A = 1$, $B = -1$. You find an extensive literature in [7].

* Research partly done while the author was a visiting professor at the Fachbereich 14 - Informatik, Universität des Saarlandes.

To establish the third and fifth powers in the Fibonacci sequence the author [5], [6] transformed the problem into the solution of certain third and fifth degree Thue equation respectively. The solutions of the Thue equations were then found by means of a computer search.

Our first result is that the transformation of (2) into a q -th degree Thue equation is possible for a wider class of recurrences. More precisely we prove

Theorem 1. *Let $q \geq 3$ be odd, $B = -1$ and $D = A^2 - 4B = p$ or $4p$ with a prime p . If $n, |x| > 1$ is a solution of (2) with n odd then there exist integers $y, z \in \mathbb{Z}$, $(y, z) = 1$ such that*

$$x^2 = y^2 + z^2$$

and

$$f(y, z) = \frac{2 - Ai}{4}(y - zi)^q + \frac{2 + Ai}{4}(y + zi)^q = \pm 1. \quad (3)$$

Generally, $f(y, z)$ is an irreducible polynomial over $\mathbb{Q}[y, z]$ and therefore it is hard to solve (3) for a given q .

For $A = 2, B = -1$ the sequence defined by (1) is called Pell sequence. We shall denote it by $\{P_n\}_{n=0}^{\infty}$. It follows from a result of Ljunggren [3] that the equation

$$P_n = x^q \quad (4)$$

has for $q = 2$ only the solutions $(n, x) = (0, 0), (1, 1)$ and $(7, 13)$. In his proof Ljunggren used complicated devices of algebraic number theory and p -adic analysis.

Combining a recent result of Wolfskill [10] with a simple computer search we give a new proof of Ljunggren's theorem. Moreover we are able to find not only the squares but all the powers in the Pell sequence.

It is clear that the pairs $(n, x) = (0, 0)$ and $(1, 1)$ are solutions of (4) for any $q \geq 2$. We call them trivial solutions.

Using Theorem 1 we prove

Theorem 2. *Equation (4) has only for $q = 2$ a non-trivial solution, namely $(n, x) = (7, 13)$.*

Erdős [1], [2] considered the equation

$$\binom{n}{k} = y^l \quad (5)$$

in positive integers k, l, n, y subject to $k \geq 2, n \geq 2k, y \geq 2, l \geq 2$. If $k = l = 2$, then (5) has infinitely many solutions, which are easy to characterize. He proved that there are no solutions with $k \geq 4$ or $l = 3$. It follows from a result of Tijdeman [9] that there is an effectively computable upper bound for the solutions of (5) with $k = 2, l \geq 3$ and $k = 3, l \geq 2$. From Theorem 2 we derive

Corollary 1. *Equation (5) has for $k = 2, l > 2$ even no solutions.*

2. Proof of Theorem 1

To prove theorem 1 we need the following

Lemma 1. *Let $D = A^2 - 4B = b^2p$, where $b, p \in \mathbb{Z}$ and p is a prime. If $(n, x) \in \mathbb{Z}^2, n$ odd is a solution of (2), then there exists $u \in \mathbb{Z}$ with*

$$b^4x^{2q} = (b^2 \pm Au)^2 - 4Bu^2. \tag{6}$$

Proof. Let α and β denote the zeros of the polynomial $X^2 - AX + B$ and put $S_n = \alpha^n + \beta^n$ for $n \geq 0$. If n is odd then it is easy to see that

$$pb^2R_n^2 = S_n^2 - 4B. \tag{7}$$

This implies $S_n^2 \equiv 4B \pmod{p}$. On the other hand $A^2 \equiv 4B \pmod{p}$, hence $S_n \equiv \pm A \pmod{p}$. Thus, there exists an $u \in \mathbb{Z}$ such that $S_n = up \pm A$ by a suitable choice of the sign. Inserting this in (7) we get

$$pb^2x^{2q} = u^2p^2 \pm 2Aup + A^2 - 4B = u^2p^2 \pm 2Aup + b^2p.$$

Dividing this equation by p and multiplying by b^2 we get

$$b^4x^{2q} = b^4 \pm 2Aub^2 + u^2b^2p = (b^2 \pm Au)^2 + u^2(b^2p - A^2) = (b^2 \pm Au)^2 - 4Bu^2.$$

The lemma is proved. ■

Proof of Theorem 1. We have

$$b = \begin{cases} 1, & \text{if } A \text{ is odd} \\ 2, & \text{if } A \text{ is even} \end{cases}$$

with the notation of Lemma 1. There exists by Lemma 1 an $u \in \mathbb{Z}$ with

$$x^{2q} = (1 \pm Au)^2 + (2u)^2, \quad (8)$$

if A is odd, and

$$16x^{2q} = (4 \pm Au)^2 + 4u^2,$$

if A is even, say $A = 2A_1$. In the last case u has to be even too, say $u = 2u_1$ and we get

$$x^{2q} = (1 \pm A_1 u_1)^2 + u_1^2. \quad (9)$$

Since $q \geq 3$, x has to be odd in both cases and (8) and (9) can be written in the common form

$$x^{2q} = v^2 + w^2, \quad (10)$$

with $v, w \in \mathbb{Z}$, $(v, w) = 1$. Further we may assume without loss of generality w even.

The right hand side of (10) can be factored in the ring of the Gaussian integers $\mathbb{Z}[i]$. These two factors must be q -th powers in $\mathbb{Z}[i]$ because they are relatively primes and the units of $\mathbb{Z}[i]$ are all q -th powers. Thus there exist $y, z \in \mathbb{Z}$ with

$$v + wi = (y + zi)^q$$

and

$$x^2 = y^2 + z^2.$$

Taking complex conjugates we get

$$v = \frac{1}{2}[(y + zi)^q + (y - zi)^q]$$

and

$$w = \frac{1}{2i}[(y + zi)^q - (y - zi)^q].$$

Consider now the case A odd. Then, by (8), u is even say $u = 2u_1$. Thus

$$u_1 = \frac{1}{8i}[(y + zi)^2 - (y - zi)^q]$$

and

$$2Au_1 \pm 1 = \frac{1}{2}[(y + zi)^q + (y - zi)^q].$$

From these two equations (3) follows immediately.

The case A even can be treated similarly, therefore we omit it. Theorem 1 is proved. ■

3. Proof of Theorem 2 and the Corollary

To prove Theorem 2 we need the following property of the sequence $\{R_n\}_{n=0}^\infty$.

Lemma 2. *Let $n > 0, m \geq 0$. Then $R_n | R_{nm}$ and*

$$\left(\frac{R_{nm}}{R_n}, R_n\right) = (m, R_n). \tag{11}$$

Proof. We use the following well known facts about recursive sequences

(i) Let $r \geq 0$ and $n, m \geq 1$ then

$$R_{nm+r} = R_n R_{n(m-1)+r+1} - BR_{n-1} R_{n(m-1)+r}. \tag{12}$$

(ii) Let $n \geq 1$, then $(R_n, R_{n-1}) = 1$.

Let now $n > 0$ and $m \geq 0$ then we have

$$R_{nm+1} \equiv (-BR_{n-1})^m \pmod{R_n}. \tag{13}$$

In fact, (13) is obviously true for $m = 0, 1$. Assume that it is true for an $m \geq 1$. Taking $r = 1$ in (12) and using the induction hypothesis we get

$$R_{n(m+1)+1} = R_n R_{nm+2} - BR_{n-1} R_{nm+1} \equiv (-BR_{n-1})^{m+1} \pmod{R_n},$$

which proves (13).

The first assertion, $R_n | R_{nm}$ is well known and follows easily from (12).

Let $n, m > 0$. We prove now

$$\frac{R_{nm}}{R_n} \equiv m(-BR_{n-1})^{m-1} \pmod{R_n}. \tag{14}$$

This is obviously true for $m = 1$. Assume (14) is true for an $m \geq 1$. Taking $r = 0$ in (12), using the induction hypothesis and (13) we get

$$\begin{aligned} \frac{R_{n(m+1)}}{R_n} &= R_{nm+1} - BR_{n-1} \frac{R_{nm}}{R_n} \equiv (-BR_{n-1})^m + m(-BR_{n-1})^m \\ &= (m+1)(-BR_{n-1})^m \pmod{R_n}. \end{aligned}$$

Hence (14) is true for any $n, m > 0$.

It is obvious that (11) is true for $m = 0$. Let $m > 1$, then by (14), (ii) and by $B = \pm 1$ we have

$$\left(\frac{R_{nm}}{R_n}, R_n\right) = (m(-BR_{n-1})^{m-1}, R_n) = (m, R_n).$$

The lemma is proved. ■

Lemma 3. Let $q \geq 2, n \geq 0$ and assume that P_n is a q -th power. Then either $n = 0, 1$ or there exists a prime $p \geq 3$ such that $p|n$ and P_p is also a q -th power.

Proof. It is easy to see that any prime divisors of P_r , where r is a prime, is greater than r . Let $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ with $p_1 < \dots < p_r$ primes.

Assume that $p_r \geq 3$. Then any prime divisors of P_{p_r} are larger than p_r , hence $(P_{p_r}, \frac{n}{p_r}) = 1$. As $(\frac{P_n}{P_{p_r}}, P_{p_r}) = 1$ by Lemma 2, any prime factors of P_{p_r} , occur in P_n in the same power as in P_{p_r} , hence P_{p_r} is a q -th power too.

Let $n = 2^\alpha$. As $P_4 = 12 = 4 \cdot 3$ exactly the first power of 3 divides P_{2^α} for $\alpha \geq 2$, so they can not be q -th powers for $q \geq 2$. Finally $P_2 = 2$, proves the lemma completely. ■

Proof of Theorem 2. Consider first the case $q = 2$. Wolfskill [10] (Example 1, p. 137) proved that if (4) holds for an odd n , then $n \leq 469$. Using this bound and the sieve procedure described in [5] it is easy to check that the only solutions of (4) with n odd are $n = 1$ and 7.

Hence if (4) holds then $n = 2^\alpha \cdot 7^\beta$ with $\beta \geq 1$ by Lemma 3. But $P_{14} = 2 \cdot 13^2 \cdot 239$ so, by Lemma 2, exactly the first power of 239 divides $P_{2^\alpha \cdot 7^\beta}$ for $\beta \geq 1$ and hence they can not be squares. This proves the theorem for $q = 2$.

Let $q > 2$, even. Then as $P_7 = 13^2$ equation (4) is solvable only for $n = 0$ and 1.

Let $q > 2$ be an odd prime. We prove that the only solution of (4) with n odd is $n = 1$ which implies the assertion of the theorem by means of Lemma 3.

Let n, x be a solution of (4) with n an odd prime. There exist by Theorem 1 integers y, z with

$$x^2 = y^2 + z^2 \quad (15)$$

$$f_q(y, z) = \frac{1-i}{2}(y-zi)^q + \frac{1+i}{2}(y+zi)^q = \pm 1. \quad (16)$$

Let $q = 4k + 3$ with $k \in \mathbb{Z}$. Then

$$\begin{aligned} f_q(-1, 1) &= \frac{1+i}{2}(-1+i)^q + \frac{1-i}{2}(-1-i)^q \\ &= \frac{(1+i)(-1+i)}{2}(-1+i)^{2(2k+1)} - \frac{(1-i)(1+i)}{2}(1+i)^{2(2k+1)} \\ &= -(-2i)^{2k+1} - (2i)^{2k+1} \\ &= 0. \end{aligned}$$

This means $\frac{y}{z} + 1 | z^q f_q(\frac{y}{z}, 1)$, which is equivalent to

$$y + z | f_q(y, z).$$

Similarly, if $q = 4k + 1$ with a $k \in \mathbb{Z}$, then we have

$$f_q(1, 1) = 0,$$

hence $y - z | f_q(y, z)$ in this case.

The divisibility relations together with (16) imply $|y+z| = 1$ or $|y-z| = 1$. Thus $y = \pm(z \pm 1)$. Inserting this value into (15) we get

$$x^2 = z^2 + (z \pm 1)^2 = 2z^2 \pm 2z + 1,$$

or equivalently

$$(2z \pm 1)^2 - 2x^2 = -1.$$

The pair $(x, z) \in \mathbb{Z}^2$ is a solution of the last equation if and only if there exists an $m \in \mathbb{Z}$ such that

$$x = \pm P_{2m+1}.$$

Hence, by (4) $P_n = \pm(P_{2m+1})^q$, which means that $P_{2m+1} | P_n$ for $2m+1 < n$. This contradicts the primality of n . Thus (4) has no solutions with n prime, and so by Lemma 3 no solutions with $n \geq 2$. Theorem 2 is proved. ■

Remark 1. *If $q \equiv 3 \pmod{4}$ then it is possible to prove that (16) has the only solutions $(y, z) = (0, \pm 1), (\pm 1, 0)$. For $q \equiv 1 \pmod{4}$ I am able to prove that $yz | \frac{q-1}{2}$ which together with the condition $|y-z| = 1$ implies the same result only for small values of q .*

Proof of Corollary. Let $k = 2$ and $n, y, l \in \mathbb{Z}$ be a solution of (5) with $l = 2q, q \geq 2$. Then (5) implies

$$(2n - 1)^2 - 2(2y^q)^2 = 1.$$

It follows from the theory of Pellian equations that there exists an $u \geq 0$ such that

$$2y^q = P_{2u}. \tag{17}$$

As $y \geq 2$ we have $u \geq 2$. Let p be the greatest prime divisor of u . If $p \geq 3$ then any prime divisors of P_p are larger than p and it must be a q -th power by (11) and (17). By Theorem 2 this is possible only if $q = 2$ and $u = 7$. But $P_{14} = 2 \cdot 13^2 \cdot 239$ gives no solutions of (17).

We have seen in the proof of Lemma 3 that exactly the first power of 3 divides P_{2^α} for $\alpha \geq 2$ which proves that (17) has no solutions also for $p = 2$. ■

References

- [1] P. Erdős, Note on the product of consecutive integers (I) and (II), *J. London Math. Soc.* **14**(1939), 194–198 and 245–249.
- [2] P. Erdős, On a diophantine equation, *J. London Math. Soc.* **26**(1951), 176–178.
- [3] W. Ljunggren, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, *Avh. Norske Vid. Akad. Oslo* **5**(1942).
- [4] A. Pethő, Perfect powers in second order linear recurrences, *J. Number Theory* **15**(1982), 5–13.
- [5] A. Pethő, Perfect powers in second order recurrences, in: *Topics in Classical Number Theory*, Akadémiai Kiadó, Budapest, 1981, 1217–1227.
- [6] A. Pethő, Full cubes in the Fibonacci sequences, *Publ. Math. Debrecen* **30**(1983), 117–127.
- [7] S. Rabinowitz, About the form of Fibonacci numbers, preprint from 8.27.1990.
- [8] T.N. Shorey and C.L. Stewart, On the diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrences, *Math. Scand.* **52**(1983), 24–36.
- [9] R. Tijdeman, Applications of the Gel'fond-Baker method to rational number theory, in: *Topics in Number Theory*, Coll. Math János Bolyai, **13**, North-Holland, Amsterdam, 1976, 399–416.
- [10] J. Wolfskill, Bounding squares in second order recurrence sequences, *Acta Arith.* **54**(1989), 127–145.

Attila Pethő

Kossuth Lajos University
Department of Computer Science
H-4010 Debrecen, P.O.Box 12
Hungary