Squares in binary recurrence sequences

K. Nakamula
Department of Mathematics
Tokyo Metropolitan University
and
A. Pethő*
Laboratory of Informatics
University Medical School Debrecen,
Nagyerdei krt. 98.
H-4028 Debrecen
Hungary

November 28, 2009

Let a, b be integers, $d = a^2 + 4b$

$$\alpha = \frac{a + \sqrt{d}}{2}, \qquad \beta = \frac{a - \sqrt{d}}{2}$$

and

$$u_n(a,b) = u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad v_n(a,b) = v_n = \alpha^n + \beta^n,$$

with $n \geq 0$ integer.

If $a = b = 1$, then u_n and v_n become the well known Fibonacci and Lucas sequence respectively. Cohn [C1] and independently Wyler [W] proved in this case that u_n is a square if and only if $n = 0, 1, 2$ or 12. Cohn generalized this result, see [C2, C3].

Recently Mc Daniel and Ribenboim [McR] proved that if a and b are odd and relatively prime and u_n is a square or double of a square then $n \leq 12$. In the proof of the above results congruence properties of the sequence u_n were used.

*Research supported in part by Hungarian National Foundation for Scientific Research Grant 1641/95.

Mignotte and Pethő [MP] applied a completely different approach to prove that if $b = -1$ and $n > 4$ then $u_n = w\Box$ is impossible with $w \in \{1, 2, 3, 6\}$, moreover these equations have solutions for $n = 4$ only if $a = 338$ in which case $u_4 = (2 \cdot 13 \cdot 239)^2$.

Extending the method of Mignotte and Pethő we are intended to prove in this paper the following theorems.

Theorem 1 *Let $b = 1$. If*

$$u_n = w\Box \tag{1}$$

with $w \in \{1, 2, 3, 6\}$ then $n \leq 2$ except when $(a, n, w) = (1, 12, 1), (1, 3, 2), (1, 4, 3), (1, 6, 2), (2, 4, 3), (2, 7, 1), (4, 4, 2)$.

Theorem 2 *Let a be even or a square and $b = 1$. If*

$$v_n = w\Box \tag{2}$$

with $w \in \{1, 2, 3, 6\}$ then $n \leq 1$.

Theorem 3 *Let $b = -1$. If*

$$v_n = w\Box \tag{3}$$

with $w \in \{1, 2, 3, 6\}$ then $n \leq 1$ except when $(a, n, w) = (1, 2, 3), (1, 3, 1), (1, 6, 2), (2, 2, 6), (3, 3, 36)$.

1 Elementary properties of u_n and v_n.

In this section we shall prove that it is enough to solve equations (1),(2) and (3) only for $w = 1$ and n odd. We shall use the same method as Mignotte and Pethő [MP]. For a prime p and non-zero integer n let $w_p(n)$ denote the highest power of p dividing n.

Lemma 1 *Let p be a prime, a an integer and $b = \pm 1$.*

1. *If $p \geq 5$ and $p \not| d$, then any prime divisor of u_p and v_p is larger then p.*

2. *If $p | d$ then*

(a) $p|u_p$,

(b) *if* $p \neq 2$ *then* $p \not| v_n$ *for all* n,

(c) *if* $p = 2$ *then* $w_2(v_n) = 1$ *for all* n.

Proof: The proof of 1. is very similar to the proof of Lemma 2 of [MP], therefore we omit it.

Assume that $p|d$ and consider the sequence u_n. From $p|d$ it follows $\alpha \equiv \beta \pmod p$ and so $\beta^2 \equiv \alpha\beta \equiv -b \pmod p$. An easy induction argument shows that $u_n \equiv n\beta^{n-1} \pmod p$, which implies $p|u_p$.

If $p \neq 2$ and $p|d$ then $\alpha \equiv \beta \pmod p$ implies $v_n \equiv 2\alpha^n \pmod p$, thus p never divides v_n.

Finally if $2|d$, then a is even and so $4|d$. Hence $v_n \equiv 2\alpha^n \pmod 4$. The lemma is proved. □

Lemma 2 *Let* n *be an integer such that its largest prime divisor* q *is greater then* 3. *If* $u_n = w\square$ *or* $v_n = w\square$ *with* $w \in \{1,2,3,6\}$ *then* $u_q = \square$ *or* $u_{q^2} = \square$ *or* $v_q = \square$ *or* $v_q = 2\square$ *respectively. The last case can occour only if* a *is even.*

Proof: The proof is the same as of the proof of Lemma 3. of [MP], except that if a is even and $v_n = w\square$ then we have to work with $\frac{v_n}{2}$ instead of v_n. □

Lemma 3 *Let* $n = 2^s \cdot 3^t$, *where* $s,t \geq 0$ *and* $s+t \geq 2$. *Then there exist a prime* $p \geq 5$ *such that* $w_p(u_n)$ *is odd except when* $(a,n) = (1,3), (1,4), (1,6), (1,12), (2,4), (4,4)$.

Proof: We consider (1) with $n = 4, 6$ and 9 and $w \in \{1,2,3,6\}$ separatively. The letters x, y will denote unknown integers.

Let $n = 4$, then $u_4 = a(a^2+2)$. Remark that $(a, a^2+2) = 1$ or 2 according as a is odd or even.

The subcase $u_4 = \square$ and a odd is impossible. Indeed, if a is even then we get $a = 2x^2$ and $a^2+2 = 2y^2$, which implies $y^2 = 2x^4+1$. This equation has the only solution $x = 0, y = 1$ by Ljungreen [L], hence $u_4 = \square$ does not have solution.

If $u_4 = 2\square$, then a must be even, say $a = (2x)^2$ and $a^2+2 = 2y^2$, hence $8x^4 = y^2-1 = (y-1)(y+1)$. This implies $2u^4 - v^4 = \pm 1$, with $uv = x$. The only solutions of this equation is $u = v = 1$ and $u = 0, v = 1$ by Ljungreen [L]. In the first case $a = 0$, which is not interesting, while in the second case we get $a = 4$, $u_4(4) = 2 \cdot 6^2$. One can easily check that $u_8(4) = 7 \cdot 23 \cdot 12^2$

and $u_{12}(4) = 17 \cdot 19 \cdot 107 \cdot 6^3$, hence $u_{2^\alpha m}(4)$ for $\alpha \geq 3$ and $u_{2^\alpha 3^\beta m}$ with $\alpha \geq 2$, $\beta \geq 1$ has a prime divisor in odd power.

If $u_4 = 3\square$ and $3|a$ then $a^2 + 2 = \square$, which is impossible. Otherwise, if $3 \not| a$ then $a^2+2 = 3x^2$ and $a = y^2$, i.e. $y^4 - 3x^2 = -2$ if $2 \not| a$ or $a^2+2 = 6x^2$ and $a = 2y^2$, i.e. $2y^4 - 3x^2 = -1$ if $2|a$. We have in both cases the non-trivial solution $(x, y) = (1, 1)$, in the first case $a = 1$, $u_4(1) = 3$, while in the second one $a = 2$, $u_4(2) = 12$. It is easy to see that $u_8(2) = 3 \cdot 17 \cdot 2^3$ and $u_{12}(2) = 5 \cdot 7 \cdot 11 \cdot 6^2$ and $u_8(1) = 3 \cdot 7$, $u_{12}(1) = 144 = 12^2$ and $u_9(1) = 34 = 2 \cdot 17$.

Let $u_4 = 6\square$, then a is even. If $3 \not| a$ then as $w_2(a^2 + 2) = 1$ we get $a = (2y)^2$ and $8y^4 + 1 = 3x^2$, but this equation is impossible mod 4. If $3|a$ then $a = 3(2y)^2$ and $a^2 + 2 = 2x^2$, thus $x^2 - 2(6y^2)^2 = 1$. The theory of Pell's equation implies that

$$6y^2 = \frac{(3+2\sqrt{2})^m - (3-2\sqrt{2})^m}{2\sqrt{2}}$$

with a non-negative integer m, or equivalently

$$3y^2 = \frac{(3+2\sqrt{2})^m - (3-2\sqrt{2})^m}{4\sqrt{2}} = u_m(6, -1).$$

By the Theorem of [MP] $m \leq 3$, thus $y = 0$ which leads to $a = 0$.

Let now $n = 6$, then $u_6 = u_3 \cdot v_3 = (a^2 + 1)a(a^2 + 3)$. Remark that $(u_3, v_3) = 2$ if a is odd and 1 if a is even. It is clear that $a^2 + 1 = \square$ has only the solution $a = 0$ while $a^2 + 1 = 3\square$ and $a^2 + 1 = 6\square$ is impossible modulo 3. Thus we have to consider only those cases, when $a^2 + 1 = 2\square$. This relation implies $3 \not| a$, thus $3 \not| v_3$ and either $v_3 = \square$ of $v_3 = 2\square$. If $v_3 = a(a^2 + 3) = \square$, then as $3 \not| a$ we have $a = \square$ and $a^2 + 3 = \square$, which holds only if $a = 1$, $u_6(1) = 8$. If $v_3 = 2\square$, then $a = \square$ and $a^2 + 3 = 2\square$, which is impossible mod 3.

Finally let $n = 9$. A simple calculation shows that $u_9 = u_3(du_3^2 - 3)$. If $u_9 = w\square$ vith $w \in \{1, 2, 3, 6\}$, then $u_3 = w\square$, which is possible only if $w = 2$ and $3 \not| a$. Hence 3 does not divide $du_3^2 - 3$ and as u_3 is even only $du_3^2 - 3 = \square$ can eventually occur. From $u_3 = a^2 + 1 = 2\square$ follows $a^2 \equiv 1$ or 4, i. e. $du_3^2 - 3 = (a^2 + 4)(a^2 + 1)^2 - 3 \equiv 2$ modulo 5, which contradicts $du_3^2 - 3 = \square$.

The lemma is completely proved □

2 Main preparatory lemmata.

We solve in this section completely equations $(1), (2)$ and (3) under the assumptions $w = 1$ and n odd. The method is the same in each cases and consists of three steps: First we transform the equations to find appropriate units in orders of infinite families of quartic algebraic number fields. In the second step we establish the basis of the unit group of the orders. We are able to do this for (2) only if a is even or a square. This is the reason of the assumptions in Theorem 2. In the last step we are using analytical considerations. For (3) this is easy, while in the other cases combinations of lower bounds for linear form in logarithms of algebraic numbers and numerical diophantine approximation techniques lead to the result.

Lemma 4 *Equation*

$$u_m(a,1) = x^2 \tag{4}$$

with $x \in \mathbb{Z}, m \geq 3$ *odd holds if and only if* $(a, m, x) = (2, 7, 13)$.

Proof: Put $m = 2k + 1$. As $u_3 = a^2 + 1$ is for $a > 0$ never a square we may assume $k \geq 2$. Moreover we may obviously assume $x > 0$. Multiplying (4) by $\alpha\sqrt{d}$ we get

$$\alpha^{2(k+1)} + \beta^{2k} = \alpha\sqrt{d}x^2, \tag{5}$$

which implies

$$\beta^{2k} = (\alpha^{k+1} - \vartheta x)(\alpha^{k+1} + \vartheta x),$$

with $\vartheta = \sqrt{\alpha\sqrt{d}}$. Hence $\alpha^{k+1} + \vartheta x = \varepsilon$ is a unit in $\mathbb{Z}[\vartheta, \alpha]$.

The field $\mathbf{Q}(\vartheta)$ is a cyclic quartic number field. Putting $\vartheta' = \sqrt{-\beta\sqrt{d}}$ the homomorphism $\sigma : \mathbf{Q}(\vartheta) \to \mathbf{C}$ with the property $\vartheta^\sigma = \vartheta'$ generates the Galois group of $\mathbf{Q}(\vartheta)$ over $\mathbf{Q}$. For $\gamma \in \mathbf{Q}(\vartheta)$ let in the sequel $\gamma^{(i)} = \gamma^{\sigma^i}$ for $i = 1, \ldots, 4$, i.e. let $\gamma^{(i)}$ be the i-th conjugate of γ.

The group $\xi =< -1, \alpha, \vartheta - 1, \vartheta' - 1 >$ has by Theorem 1a index at most 2 in the group of units of $\mathbb{Z}[\vartheta, \alpha]$. We can easily express the regulator R of this system of units as

$$R = 2\log\alpha\left[\log^2(\alpha(\vartheta' + 1)) + \log^2\frac{\alpha}{\vartheta + 1}\right],$$

thus we have

$$R > 2\log\alpha\log^2 2\alpha.$$

There exist $u_0 \in \{0,1\}, u_1, u_2, u_3 \in \mathbf{Q}$ with denominator at most 2 such that

$$\varepsilon = (-1)^{u_0}\alpha^{u_1}(\vartheta - 1)^{u_2}(\vartheta' - 1)^{u_3}. \tag{6}$$

The following estimates can be checked easily by inserting the given values of the defining polynomial of the accouring algebraic numbers, as well as by using elementary properties of the logarithm function.

$$\begin{array}{rll}
a + \dfrac{1}{a+1} & \leq \alpha & \leq a + \dfrac{1}{a} \\
-\dfrac{1}{a} & \leq \beta & \leq -\dfrac{1}{a+1} \\
a + \dfrac{1}{a} & < \vartheta & \leq \alpha + \dfrac{1}{\alpha} \\
1 + \dfrac{1}{4a^2} & < \vartheta' & < 1 + \dfrac{1}{a^2} \\
\log a + \dfrac{1}{a(a+1)} & < \log\alpha & < \log a + \dfrac{3}{2a^2} \\
-\log(a+1) & < \log|\beta| & < -\log a \\
\log a + \dfrac{1}{a^2} & < \log\vartheta & < \log\alpha + \dfrac{3}{2a^2} \\
\dfrac{1}{4a^2} & < \log\vartheta' & < \dfrac{3}{2a^2}
\end{array}$$

From (5) we have

$$\vartheta x = \alpha^{k+1}\sqrt{1 + \beta^{4k+2}},$$

hence

$$\frac{1}{3}|\beta|^{3k+1} \leq \vartheta x - \alpha^{k+1} \leq \frac{1}{2}|\beta|^{3k+1}.$$

Using this inequality we can easily derive the following estimates for the conjugates of ε:

$$
\begin{aligned}
2\alpha^{k+1}+\frac{1}{3}|\beta|^{3k+1} &\le \varepsilon^{(1)}=\vartheta x+\alpha^{k+1} &&\le 2\alpha^{k+1}+\frac{1}{2}|\beta|^{3k+1} && (7)\\
\alpha^{k}-|\beta|^{k} &\le \varepsilon^{(2)}=\vartheta' x+\beta^{k+1} &&\le \alpha^{k}+|\beta|^{k} && (8)\\
-\frac{1}{2}|\beta|^{3k+1} &\le \varepsilon^{(3)}=-\vartheta x+\alpha^{k+1} &&\le -\frac{1}{3}|\beta|^{3k+1} && (9)\\
-\alpha^{k}-|\beta|^{k} &\le \varepsilon^{(4)}=-\vartheta' x+\beta^{k+1} &&\le -\alpha^{k}+|\beta|^{k} && (10)
\end{aligned}
$$

From (7) and (9) we get

$$(4k+2)\log\alpha-\log 1.5<\log\varepsilon^{(1)}-\log|\varepsilon^{(3)}|<(4k+2)\log\alpha+\frac{1}{4}|\beta|^{4k+2},$$

which is equivalent with

$$(4k+2)\log\alpha-\log 1.5<u_2\log\frac{\vartheta-1}{\vartheta+1}+u_3\log\frac{\vartheta'-1}{\vartheta'+1}<(4k+2)\log\alpha+\frac{1}{4}|\beta|^{4k+2}$$

by (6).

Similarly, inequalities (8) and (10) imply

$$|\log|\varepsilon^{(2)}|-\log|\varepsilon^{(4)}||<3|\beta|^{2k}.$$

Computing the conjugates of ε form (6) and inserting the result we get

$$\left|u_2\log\frac{\vartheta'+1}{\vartheta'-1}+u_3\log\frac{\vartheta-1}{\vartheta+1}\right|<3|\beta|^{2k},$$

which can reformulate as

$$|\Lambda|=\left|2u_2\log\alpha(\vartheta'+1)-2u_3\log\frac{\vartheta+1}{\alpha}\right|<3|\beta|^{2k}. \qquad (11)$$

We just proved two, in u_2 and u_3, linear inequalities. They imply that both u_2 and u_3 are negative, moreover

$$u_3>-\left(1+\frac{3}{a^3}\right)(2k+1). \qquad (12)$$

We prove now that $|u_2|$ is very small in comparing with $|u_3|$. Indeed the following chain of inequalities

$$\begin{aligned} \frac{2|u_3|}{a} > 2|u_3|\log\frac{\vartheta+1}{\alpha} &> 2|u_2|\log\alpha(\vartheta'+1)-|\Lambda| \\ &> 2|u_2|\log 2\alpha - 3\beta^{2k} \\ &> 2|u_2|\log 2a \end{aligned}$$

implies

$$|u_3| > |u_2| a \log 2a, \tag{13}$$

whenever $u_2 \neq 0$.

Consider first the case when $u_2 = 0$. Then as $\log\frac{\vartheta+1}{\alpha} > \log\frac{\alpha+1}{\alpha} > \frac{\alpha-1}{\alpha^2}$ inequality (12) can hold only if $u_3 = 0$ holds too. Then ε belongs to $\mathbf{Q}(\alpha)$ and $x = 0$.

Hence we may assume $u_2 \neq 0$ in the sequel.

To prove an upper bound for a and afterward for $|u_3|$ we shall use Theorem 2. from Laurent, Mignotte and Nesterenko [LMN]:

Theorem 4 *Let α_1, α_2 be real algebraic numbers of absolute value at least 1 and b_1, b_2 be integers. Put*

$$\tilde{\Lambda} = b_2 \log\alpha_1 - b_1 \log\alpha_1$$

and

$$D = [\mathbf{Q}(\alpha_1,\alpha_2):\mathbf{Q}]/[\mathbb{R}(\alpha_1,\alpha_2):\mathbb{R}].$$

Let a_1, a_2 and h be positive real numbers and $\rho > 1$. Put $\lambda = \log\rho$ and assume that

$$\begin{gathered} h > \max\left\{\frac{D}{2}, 5\lambda, D\left(\log\left(\frac{b_1}{a_2}+\frac{b_2}{a_1}\right)+\log\lambda+1.56\right)\right\}, \\ a_i \geq \max\{2, 2\lambda, \rho|\log\alpha_i| - \log|\alpha_i| + 2Dh(\alpha_i)\}, (i=1,2). \end{gathered}$$

If α_1 and α_2 are multiplicatively independent, then

$$\begin{aligned} \log|\tilde{\Lambda}| \geq & -\frac{\lambda a_1 a_2}{9}\left(\frac{4h}{\lambda^2}+\frac{4}{\lambda}+\frac{1}{h}\right)^2 - \frac{2\lambda}{3}(a_1+a_2)\left(\frac{4h}{\lambda^2}+\frac{4}{\lambda}+\frac{1}{h}\right) \\ & -\frac{16\sqrt{2a_1a_2}}{3}\left(1+\frac{h}{\lambda}\right)^{3/2} - 2(\lambda+h) - \log\left(a_1a_2\left(1+\frac{h}{\lambda}\right)^2\right) \\ & +\frac{\lambda}{2} + \log\lambda - 0.15. \end{aligned}$$

To apply Theorem 2.1 we chose $\alpha_1 = \alpha(\vartheta' + 1), \alpha_2 = \frac{\vartheta+1}{\alpha}, b_1 = 2u_3$ and $b_2 = 2u_2$. Remember, that both u_2 and u_3 are negative.

Put $\rho = 15, \lambda = \log 15, D = 4$,

$$a_1 = \begin{cases} 16 \log 2a + \frac{7}{a}, & \text{if } a > 10^4 \\ 169 > 17 \cdot \log(2 \cdot 10^4), & \text{if } a \le 10^4, \end{cases}$$

$$a_2 = \begin{cases} 2 \log 2a + \frac{20}{a}, & \text{if } a > 10^4 \\ 40 > 2 \log 2a + 20, & \text{if } a \le 10^4. \end{cases}$$

and

$$h = \begin{cases} 4 \log\left(\frac{-2u_3}{a_2}\right) + 12.628, & \text{if } a > 10^4 \\ 4 \log\left(\frac{-2u_3}{a_2}\right) + 13.8, & \text{if } a \le 10^4 \text{ and } -u_3 \ge 8. \end{cases}$$

One can easily check that our choice of h and a_i satisfy the conditions of Theorem 2.1. Let us consider first the case $a > 10^4$. Then putting $y = \log\left(\frac{-2u_3}{a_2}\right)$ we get by Theorem 2.1.

$$\begin{aligned} -\log|\Lambda| &< 23a_2 \log 2a(y+3.9)^2 + 36a_2(y+3.9) \\ &+ 38.5a_2(y+3.84)^{3/2} + 8y + 31.4 + \log(a_2(y+3.84)^2). \end{aligned}$$

On the other hand (12) and (13) imply

$$-\log|\Lambda| > (2k+1)\log a - \log 3a > \left(1 + \frac{3}{a^3}\right)^{-1} (-u_3) \log a - \log 3a \quad (14)$$

for all $a \ge 1$. Combining the last two inequalities, multiplying them by $2\left(1 + \frac{3}{a^3}\right)$ and dividing by $a_2 \log a$ we get:

$$\begin{aligned} &51.06(y+3.9)^2 + 7.9(y+3.9) + 4.2(y+3.84)^{3/2} + 0.1y \\ &\qquad 0.03 \log(y+3.84) + 0.5 > \exp(y), \end{aligned}$$

which implies

$$\frac{-2u_3}{a_2} < 9824.1. \quad (15)$$

We have $|2u_3| > a \log 2a$ by (14), hence

$$a \log 2a < 9824.1 \left(2 \log 2a + \frac{20}{a}\right).$$

Thus for $a > 17866$ inequality (12) has no solution, i.e. the Lemma is proved in this range.

If $10^4 < a \leq 17866$ then (16) implies

$$|2u_3| < 1.8 \cdot 10^5.$$

Finally, if $1 \leq a \leq 10^4$, then the lower bound for $|\Lambda|$ becomes

$$\begin{aligned} -\log|\Lambda| < \quad & 242.1a_2(y+4.2)^2 + 20.6a_2(y+4.2) \\ & +27.84a_2(y+4.13)^{3/2} + 8y + 40.42 + 2\log(y+4.13) \end{aligned}$$

Comparing this inequality again with (15) we get

$$\begin{aligned} 1937(y+4.2)^2 + 165(y+4.2) + 223\cdot(y+4.13)^{3/2} + 1.6y & \\ +8.1 + 0.4\log(y+4.13) & \quad > \exp(y), \end{aligned}$$

which implies

$$|2u_3| < 2.5 \cdot 10^7 \tag{16}$$

by the choice of a_2.

To prove the theorem in the range $1 \leq a \leq 17866$ we used the following reduction procedure. From (12) we get

$$\left|2u_2 - 2u_3\frac{\log\alpha_2}{\log\alpha_1}\right| < \frac{3}{\alpha^{2k}\log 2a}. \tag{17}$$

We proved also $-2.5 \cdot 10^7 < 2u_3 < 0$, if $1 \leq a \leq 17866$. Let $\frac{p}{q}$ be a convergent of $\frac{\log\alpha_2}{\log\alpha_1}$ such that $q > 2.5 \cdot 10^7$, then by a well known property of the continued fractions we get

$$\left|p - q\frac{\log\alpha_2}{\log\alpha_1}\right| < \left|2u_2 - 2u_3\frac{\log\alpha_2}{\log\alpha_1}\right| < \frac{3}{\alpha^{2k}\log 2a}.$$

Computing for each a from the range $1 \leq a \leq 17866$ the first convergent $\frac{p(a)}{q(a)}$ of the continued fraction expansion of $\frac{\log\alpha_2(a)}{\log\alpha_1(a)}$ such that $q(a) > 2.5\cdot 10^7$ and then the value

$$\left|p(a) - q(a)\frac{\log\alpha_2(a)}{\log\alpha_1(a)}\right| = \Theta(a)$$

we find a, hopefully smaller, new upper bound for k, which implies by (13) a new upper bound for $|2u_3|$. We expect, that iterating eventually this process we find that for most of the values of a inequality (12) can not hold.

This indeed happened. Unfortunatelly we can not recapitulate here the computation for all values, we only give the most important data for the case $a = 2$. The 17-th convergent of the continued fraction expansion of $\frac{\alpha_2(2)}{\alpha_1(2)}$ is $\frac{17012895}{68139853}$ and $\Theta(2) = 2.88210^{-7}$, hence $k \leq 3$. A simple calculation showes that $k = 3$, i.e. $m = 7$ is indeed a solution. For $a > 2$ we got $k \leq 1$ after the reduction, which proves the lemma. □

3 Proof of the Theorems

Proof of Theorem 1. Assume that (1) holds for an $n > 0$. If the largest prime divisor q of n is greater then 3 then $u_q = \square$ or $u_{q^2} = \square$ by Lemma 1.2. This is possible by Lemma 2.1 only if $a = 2$ and $m = 7$. As $u_5(2) = 29, u_{14}(2) = 2 \cdot 239 \cdot 13^2, u_{21}(2) = 5 \cdot 13^2 \cdot 45697$ and $u_{49}(2) = 13^2 \cdot 293 \cdot 40710764977973$ we see that if 7 is the largest prime factor of n and $n/7 > 1$ then $u_n(2)$ has always a prime factor, which is larger then 2, on the first power. Hence it remains to examine the cases when $n = 2^\alpha 3^\beta$ with $\alpha, \beta \geq 0$. But this was already done in Lemma 1.3. Theorem 1 is proved. □

References

[C1] J.H.E Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **39** (1964), 537–540.

[C2] J.H.E Cohn, *Eight Diophantine equations*, Proc. London Math. Soc., **16** (1966), 153–166.

[C3] J.H.E Cohn, *The Diophantine equation $y^2 = Dx^4 + 1$*, J. London Math. Soc. **42** (1967), 475–476.

[L] W. Ljungreen, *Zur Theorie der Gleichung $x^2+1 = Dy^4$,* Avh. Norske Vid. Akad. Oslo, No. 5 **1** (1942).

[LMN] M. Laurent, M. Mignotte et Y. Nesterenko, *Formes linéaires en deux logarithmes et dèterminants d'interpolation*, J. Number Theory, to appear.

[McR] W.L. McDaniel and P. Ribenboim, *Squares and double squares in Lucas sequences*, C.R. Math. Rep. Acad. Sci. Canada, **14** (1992), 104–108.

[MP] M. Mignotte et A. Pethő *Sur les carrés dans certaines suites de Lucas*, Sém. Théorie Nombr. Bordeaux **5** (1993), 333–341.

[W] O. Wyler *Solution to problem* 5080, Amer. Math. Monthly **71** (1964), 220–222.