Powers in the Lucas sequence when the index is divisible by three

Mª Dolores López[a,], Javier Rodrigo[b]

[a]Departamento de Matemática e Informática Aplicadas a la Ingeniería Civil de la E.T.S.I. Caminos, Canales y Puertos, Universidad Politécnica de Madrid marilo.lopez@ upm.es

[b]Departamento de Matemática Aplicada, E.T.S. de Ingeniería, Universidad Pontificia Comillas de Madrid

*Corresponding author: Mª Dolores López, Departamento de Matemática e Informática Aplicadas a la Ingeniería Civil de la E.T.S.I. Caminos, Canales y Puertos, Universidad Politécnica de Madrid, c/ Profesor Aranguren s/n, Madrid 28040, Spain

Tf: 34- 913366669; Fax: 34-913366782

Abstract:

In this paper the *m*-powers with $m \geq 2$ included in the Lucas sequences when the index satisfies some conditions are found.

Keywords: Number theory, Lucas sequences, Diophantine equations.

1. Introduction

The Lucas and companion Lucas sequences have been widely studied in the scientific literature as a natural extension of the so called Fibonacci sequence. They are defined inductively by: $U_0^{P,Q} = 0$, $U_1^{P,Q} = 1$, $U_n^{P,Q} = P\,U_{n-1}^{P,Q} - Q\,U_{n-2}^{P,Q}$ and $V_0^{P,Q} = 2$, $V_1^{P,Q} = P$, $V_n^{P,Q} = P\,V_{n-1}^{P,Q} - Q\,V_{n-2}^{P,Q}$ respectively, where P, Q are integer numbers (the Fibonacci sequence is the particular case of $U_n^{P,Q}$ with $P = 1$, $Q = -1$. The indices P, Q will be omitted when they are not necessary).

Concretely, the search of the powers included in these sequences has deserved a special attention by the number theorist. The main results at this respect for U_n are:

- For odd relative primes P, Q, the only square in U_n with $n > 2$, $n \neq 6$ is $U_{12}^{1,-1} = 144$ (see Ribenboim, Bremner&Tzanakis)
- For P divisible by 4, there is no squares in $U_n^{P,-1}$ for positive, even numbers n when additional conditions on P are considered (Kagawa)
- The only powers in $U_n^{1,-1}$ with $n > 2$ are $U_6^{1,-1} = 8$ and $U_{12}^{1,-1} = 144$ (Bugeaud)
- The only power in $U_n^{2,-1}$ with $n > 1$ is $U_7^{2,-1} = 169$ (Cohn)

In this paper the case $P > 0$, $Q = -1$ is studied: it is proved that, for n divisible by three and satisfying some extra conditions, the powers in U_n are always attained for $P = 1$ and they are $U_6^{1,-1} = 8$ and $U_{12}^{1,-1} = 144$. To do this, the diophantine equation $U_n^{P,-1} = u^m$ with unknowns (n, P, u, m), $m \geq 2$, is related with these diophantine equations according to the different cases:

- The Catalan equation $x^m - y^2 = 1$
- The Thue equation $2\,x^m - y^m = 1$
- The equation $2\,x^2 - y^4 = 1$

The following notation applies in the paper:

- N for the set of natural numbers
- $GCD(a, b)$ for the greatest common divisor of the integer numbers a, b
- $a | b$ if the integer number a divides to the integer number b
- $a \equiv b \pmod{m}$ if a is congruent with b modulus m (that is to say, $m | b - a$)

- $\binom{n}{k}$ for the binomial coefficient.

- $e_p(n)$ for the exponent of the prime p in the factorization in prime numbers of the integer number n (if p is not a prime factor of n, it is assumed that $e_p(n)=0$).

The following two identities for U_n, V_n, U_k, V_k are used along the paper (see Kagawa):

$$2^{\frac{n}{k}-1}\left(V_n + U_n\sqrt{P^2+4}\right)=\left(V_k + U_k\sqrt{P^2+4}\right)^{\frac{n}{k}} \text{ when } k \mid n \text{ and } k,\ n \text{ are positive numbers} \quad (1)$$

$$\left(V_k\right)^2-\left(P^2+4\right)\left(U_k\right)^2=4\left(-1\right)^k \quad (2)$$

The paper is structured as follows: in section 2 the main result is stated and in section 3 some concluding remarks are given. Along section 2, k and n are positive integer numbers.

2. Development

To prove the result mentioned in the introduction, a lemma is needed:

Lemma

If $k \mid n$, then $GCD\left(\frac{U_n}{U_k}, U_k\right) \Big| \frac{n}{k}$

Proof

First it is noted that if $k \mid n$, then $U_k \mid U_n$ (see for example Ribenboim), so $\frac{U_n}{U_k}$ is an integer number and the statement makes sense. Now, the following cases appear:

1) If V_k is an odd number, then by expanding (1) it is obtained that:

$$2^{\frac{n}{k}-1}U_n=\frac{n}{k}V_k^{\frac{n}{k}-1}U_k+\binom{\frac{n}{k}}{3}V_k^{\frac{n}{k}-3}U_k^3\left(P^2+4\right)+\ldots=U_k\left(\frac{n}{k}V_k^{\frac{n}{k}-1}+f\left(U_k\right)\right), \text{ where}$$

$f(x)$ is a polynomial without independent term. Now, since $GCD\left(\frac{U_n}{U_k}, U_k\right) \Big| U_k$,

$GCD\left(\frac{U_n}{U_k}, U_k\right) \Big| \frac{U_n}{U_k} = \frac{\frac{n}{k} V_k^{\frac{n}{k}-1} + f(U_k)}{2^{\frac{n}{k}-1}}$, then $GCD\left(\frac{U_n}{U_k}, U_k\right)$ divides to U_k,

$\frac{n}{k} V_k^{\frac{n}{k}-1} + f(U_k)$, so it divides to $\frac{n}{k} V_k^{\frac{n}{k}-1} + f(U_k) - f(U_k) = \frac{n}{k} V_k^{\frac{n}{k}-1}$.

Since V_k is an odd number, it is satisfied that $GCD(V_k, U_k) = 1$ by identity (2) and then $GCD\left(\frac{U_n}{U_k}, U_k\right) \Big| \frac{n}{k}$ as desired.

2) If V_k and P are even numbers, then (1) and (2) yield respectively:

$$U_n = \frac{n}{k}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-1} U_k + \binom{\frac{n}{k}}{3}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-3} U_k^3 \frac{P^2+4}{4} + \ldots = U_k\left(\frac{n}{k}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-1} + g(U_k)\right)$$

$$\left(\frac{V_k}{2}\right)^2 - \frac{P^2+4}{4} U_k^2 = (-1)^k$$

Where $g(x)$ is a polynomial with integer coefficients and without independent term. The last identity implies that $GCD\left(\frac{V_k}{2}, U_k\right) = 1$.

Now, since $GCD\left(\frac{U_n}{U_k}, U_k\right) \Big| U_k$, $GCD\left(\frac{U_n}{U_k}, U_k\right) \Big| \frac{U_n}{U_k} = \frac{n}{k}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-1} + g(U_k)$, then $GCD\left(\frac{U_n}{U_k}, U_k\right)$ divides to $\frac{n}{k}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-1} + g(U_k) - g(U_k) = \frac{n}{k}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-1}$, so $GCD\left(\frac{U_n}{U_k}, U_k\right) \Big| \frac{n}{k}$ also in this case because $GCD\left(\frac{V_k}{2}, U_k\right) = 1$.

3) If V_k is an even number and P is an odd number, then (2) implies that U_k is an even number, so (2) can be rewritten as $\left(\frac{V_k}{2}\right)^2 - (P^2+4)\left(\frac{U_k}{2}\right)^2 = (-1)^k$ and $\frac{V_k}{2}$, $\frac{U_k}{2}$ have different parity. Identity (1) can be expressed in this case as:

$$\frac{V_n}{2}+\frac{U_n}{2}\sqrt{P^2+4}=\left(\frac{V_k}{2}+\frac{U_k}{2}\sqrt{P^2+4}\right)^{\frac{n}{k}}. \qquad (3)$$

In an analogous way to case 1), it can be seen that $GCD\left(\frac{\frac{U_n}{U_k}}{2^{e_2\left(\frac{U_n}{U_k}\right)}}, U_k\right)$ divides to $\frac{n}{k}$, so in order to prove that $GCD\left(\frac{U_n}{U_k}, U_k\right) \Big| \frac{n}{k}$, it is sufficient to see that $e_2\left(GCD\left(\frac{U_n}{U_k}, U_k\right)\right) \le e_2\left(\frac{n}{k}\right)$. Three new cases appear:

- If $\frac{n}{k}$ is an odd number, then expanding the right side of (3) and equaling the terms with $\sqrt{P^2+4}$, it is obtained that:

$\frac{U_n}{U_k}=\frac{n}{k}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-1}+\binom{\frac{n}{k}}{3}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-3}\left(\frac{U_k}{2}\right)^2\left(P^2+4\right)+\ldots+\left(\frac{U_k}{2}\right)^{\frac{n}{k}-1}\left(P^2+4\right)^{\left(\frac{n}{k}-1\right)\frac{1}{2}}$, so $\frac{U_n}{U_k}$ is an odd number regardless $\frac{U_k}{2}$ is an odd number or $\frac{V_k}{2}$ is an odd number and then $e_2\left(GCD\left(\frac{U_n}{U_k}, U_k\right)\right)=0=e_2\left(\frac{n}{k}\right)$.

-If $\frac{n}{k}$ is an even number and $\frac{V_k}{2}$ is an odd number, then $\frac{U_k}{2}$ is an even number and it is obtained in an analogous way than in the previous case that:

$$\frac{U_n}{U_k}=\frac{n}{k}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-1}+\binom{\frac{n}{k}}{3}\left(\frac{V_k}{2}\right)^{\frac{n}{k}-3}\left(\frac{U_k}{2}\right)^2\left(P^2+4\right)+\ldots+\frac{n}{k}\left(\frac{U_k}{2}\right)^{\frac{n}{k}-2}\left(P^2+4\right)^{\left(\frac{n}{k}-2\right)\frac{1}{2}}$$

Now, it is a known fact that $\dfrac{\frac{n}{k}}{GCD\left(\frac{n}{k}, i\right)}\left|\binom{\frac{n}{k}}{i}\right.$, so $e_2\left(\binom{\frac{n}{k}}{i}\right) \geq e_2\left(\frac{n}{k}\right)$ when i is an odd number. Since $\frac{U_k}{2}$ is an even number, this implies that $e_2\left(\frac{U_n}{U_k}\right) = e_2\left(\frac{n}{k}\right)$, so $e_2\left(GCD\left(\frac{U_n}{U_k}, U_k\right)\right) \leq e_2\left(\frac{n}{k}\right)$ as desired.

-If $\frac{n}{k}$ and $\frac{V_k}{2}$ are even numbers, then $\frac{U_k}{2}$ is an odd number, so $e_2\left(GCD\left(\frac{U_n}{U_k}, U_k\right)\right) \leq 1 \leq e_2\left(\frac{n}{k}\right)$, as desired.

Now the theorem is stated:

Theorem

If $GCD\left(P, \frac{n}{2}\right) = 1$ when n is an even number, n has not prime factors congruent with 1 modulus 4 and it has the factor three, then the only powers included in U_n are $U_6^{1,-1} = 8$ and $U_{12}^{1,-1} = 144$

Proof

It is satisfied that $U_n = U_3 \frac{U_n}{U_3} = \left(P^2 + 1\right)\frac{U_n}{U_3}$, with $GCD\left(\frac{U_n}{U_3}, P^2 + 1\right)\left|\frac{n}{3}\right.$ by the lemma. Hence $GCD\left(\frac{U_n}{U_3}, P^2 + 1\right)$ has not prime factors congruent with 1 modulus 4 since n has not prime factors congruent with 1 modulus 4 by hypothesis. It is also satisfied that $GCD\left(\frac{U_n}{U_3}, P^2 + 1\right)$ has not prime factors congruent with 3 modulus 4 (otherwise, -1 would be a quadratic residue modulus a prime number that is congruent with 3 modulus 4). Therefore, $GCD\left(\frac{U_n}{U_3}, P^2 + 1\right) = 1 \text{ or } 2$ (since $P^2 + 1 \equiv 2 \pmod{4}$ when $P^2 + 1$ is an even number). So, if $U_n = u^m$ with $u, m \in N$, $m \geq 2$, then the following cases must be considered:

1) If $GCD\left(\frac{U_n}{U_3}, P^2+1\right)=1$, then $U_n=\left(P^2+1\right)\frac{U_n}{U_3}=u^m$ implies that $P^2+1=v^m$ with $v\in N$, so the Catalan equation $x^m-y^2=1$ has a solution in positive integers: (v, P), a contradiction (see Mihailescu)

2) If $GCD\left(\frac{U_n}{U_3}, P^2+1\right)=2$, then n must be an even number because $GCD\left(\frac{U_n}{U_3}, P^2+1\right)=2\left|\frac{n}{3}\right.$ by the lemma, so $U_n=U_2\,U_3\,\frac{U_n}{U_2\,U_3}=P\left(P^2+1\right)\frac{U_n}{U_2\,U_3}$.

Now, $U_n=P\left(P^2+1\right)\frac{U_n}{U_2\,U_3}=u^m$ implies that $P=w^m$ with $w\in N$, $P^2+1=2\,v^m$ with $v\in N$, because $GCD\left(\frac{U_n}{U_3}, P^2+1\right)=2$ and $GCD\left(P, \frac{U_n}{U_2}\right)=1$ by the lemma and the hypothesis $GCD\left(P, \frac{n}{2}\right)=1$. Then it is satisfied that $2\,v^m-\left(w^2\right)^m=1$, so the diophantine equation $2\,x^m-y^m=1$ has a solution in positive integers: $\left(v, w^2\right)$. But for $m\geq 3$ the only solution in positive integers to this equation is $x=y=1$ (see Darmon). This implies that $w^2=1$ and then $P=w^m=1$ (P is a positive number). But in this case the only m-power with $m\geq 3$ in U_n for the required conditions on n is $U_6^{1,-1}=8=2^3$, as stated in the introduction.

For $m=2$ it is satisfied that $2\,v^2-w^4=1$, so the diophantine equation $2\,x^2-y^4=1$ has a solution in positive integers: (v, w). But the only solution in positive integers to this equation is $x=y=1$ (see M. Le). This implies that $P=w^m=1$. But in this case the only square in U_n for the required conditions on n is $U_{12}^{1,-1}=144=12^2$, as stated in the introduction and the proof is finished.

3. Concluding remarks

A result about the powers in the Lucas sequences U_n has been stated for indices n divisible by three and satisfying certain conditions. This result is very general in the sense that it has been stated for *m*-powers for every $m\geq 2$, and without restrictions on the parameter P when n is an odd number. Therefore this paper complements previous studies of Kagawa, Ribenboim about the squares in the Lucas sequences and of Bennett about the *m*-powers with $m \geq 3$ in the Lucas sequences.

A future line of work could be to relax the conditions on the index n in the theorem of section 2

References

1. M. A. Bennett, Powers in recurrence sequences: Pell equations, Transactions of the American Mathematical Society, 357 (2004), 1675–1691
2. A. Bremner and N. Tzanakis, Lucas sequences whose 12th or 9th term is a square, J. Number Theory, 107 (2004), 215-227.
3. Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches to exponential Diophantine equations, I. Fibonacci and Lucas perfect powers. Annals of Math. 163 (2006), 969-1018.
4. Cohn, J. H. E. (1996). Perfect Pell powers. Glasgow Mathematical Journal 38 (1): 19–20.
5. H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, J. Reine Angew. Math. 490 (1997), 81–100.
6. Kagawa, T. and Terai, N.: Squares in Lucas sequences and some Diophantine equations. Manuscripta Math. 96, 195–202 (1998).
7. M. Le. On the diophantine equation $(x^m + 1)(x^n + 1) = y^2$. Acta arithmetica, LXXXII.1, 17-26, 1997.
8. Mihailescu, P. Primary ciclotomic units and a proof of Catalan's conjecture; J. Reine angew.Math. 572, 167-195, 2004.
9. P. Ribenboim and W. L. McDaniel, The square terms in Lucas sequences. J. Number Theory 58 (1996), 104–122.