Miskolc Mathematical Notes
Vol. 19 (2018), No. 1, pp. 641–648

HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2018.1750

ON THE ORDER OF APPEARANCE OF THE DIFFERENCE OF TWO LUCAS NUMBERS

PAVEL TROJOVSKÝ

Received 22 September, 2015

Abstract. Let F_n be the nth Fibonacci number and let L_n be the nth Lucas number. The order of appearance $z(n)$ of a natural number n is defined as the smallest natural number k such that n divides F_k. For instance, $z(L_n) = 2n$, for all $n > 2$. In this paper, among other things, we prove that

$$z(L_m - L_n) = \frac{5F_p}{p} \cdot \frac{m^2 - n^2}{4},$$

for all distinct positive integers $m \equiv n \pmod 4$, with $\gcd(m,n) = p > 2$ prime.

2010 *Mathematics Subject Classification:* 11B39; 11A07

Keywords: Lucas number, Fibonacci number, order of appearance

1. INTRODUCTION

Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence given by $F_{n+2} = F_{n+1} + F_n$, for $n \geq 0$, where $F_0 = 0$ and $F_1 = 1$. These numbers are well-known for possessing amazing properties (consult [4] together with its very extensive annotated bibliography for additional references and history). We cannot go very far in the lore of Fibonacci numbers without encountering its companion Lucas sequence $(L_n)_{n\geq 0}$ which follows the same recursive pattern as the Fibonacci numbers, but with initial values $L_0 = 2$ and $L_1 = 1$.

The study of the divisibility properties of Fibonacci numbers has always been a popular area of research. Let n be a positive integer number, the *order (or rank) of appearance* of n in the Fibonacci sequence, denoted by $z(n)$, is defined as the smallest positive integer k, such that $n \mid F_k$ (some authors also call it *order of apparition*, or *Fibonacci entry point*). There are several results about $z(n)$ in the literature. For instance, in 1975, J. Sallé [13] proved that $z(n) \leq 2n$, for all positive integers n. This is the sharpest upper bound for $z(n)$, since for example, $z(6) = 12$ and $z(30) = 60$ (see [10] for related results). In the case of a prime number p, one has the better upper bound $z(p) \leq p + 1$, which is a consequence of the known congruence $F_{p-(\frac{p}{5})} \equiv 0$

(mod p), for $p \neq 2$, where $(\frac{a}{q})$ denotes the Legendre symbol of a with respect to a prime $q > 2$.

We remark that there is no a closed formula for $z(n)$, but by using computational methods and several calculations, one can see patterns of $z(n)$ for some positive integers n. For example, with this computational approach, Marques [7–9] found explicit formulas for the order of appearance of integers related to Fibonacci and Lucas number, such as $C_{mk}/C_k, C_m \pm 1, C_nC_{n+1}C_{n+2}$ and C_n^k, where $(C_n)_n = (F_n)_n$ or $(L_n)_n$.

In this paper, we study the order of appearance of $L_m - L_n$. Again, we used `Mathematica` to search for patterns for $z(L_m - L_n)$. We were surprised to find out that in some cases, these values are related to the sequences

$$1, 2, 5, 13, 89, 233, 1597, 4181, 28657, 514229, \ldots$$

and

$$3, 4, 11, 29, 199, 521, 3571, 9349, 64079, 1149851, \ldots.$$

A search in the On-Line Encyclopedia of Integer Sequences [14] is enough to conclude that, surprisingly, these sequences are the first few Fibonacci and Lucas numbers with prime indexes, respectively. In fact, this interpretation is confirmed by exhaustive calculations. More precisely, our main results are the following.

Theorem 1. *Let m and $n > 1$ be positive distinct integers, such that $m \equiv n$ (mod 4). We have*

(i) *If $\gcd(m,n) = 1$, then*

$$z(L_m - L_n) = \frac{5(m^2 - n^2)}{4}.$$

(ii) *If $\gcd(m,n) = p$ is prime, then*

$$z(L_m - L_n) = \frac{5F_p}{p} \cdot \frac{m^2 - n^2}{4}.$$

2. Auxiliary results

Before proceeding further, we recall some facts on Fibonacci and Lucas numbers for the convenience of the reader.

Lemma 1. *We have*

(a) *$F_n \mid F_m$ if and only if $n \mid m$.*
(b) *$L_n \mid F_m$ if and only if $n \mid m$ and m/n is even.*
(c) *$5F_n \mid F_{5n}$, for all integer n.*
(d) *If $d = \gcd(m,n)$, then $\gcd(F_m, F_n) = F_d$,*

$$\gcd(L_m, L_n) = \begin{cases} L_d, & \text{if } \nu_2(m) = \nu_2(n); \\ 1 \text{ or } 2, & \text{otherwise} \end{cases}$$

$$\text{and } \gcd(F_m, L_n) = \begin{cases} L_d, & \text{if } m/d \text{ is even and } n/d \text{ is odd;} \\ 1 \text{ or } 2, & \text{otherwise.} \end{cases}$$

(e) $F_{p-(\frac{5}{p})} \equiv 0 \pmod{p}$, *for all primes* p. *In particular,* $\gcd(F_p, p) = 1$, *if* $p \neq 5$.

(f) $L_p \equiv 1 \pmod{p}$, *for all primes* p. *In particular,* $\gcd(L_p, p) = 1$.

Here, as usual, $(\frac{a}{q})$ denotes the Legendre symbol of a with respect to a prime $q > 2$.

Proof of these assertions can be found in [4]. We refer the reader to [1,3,6,11] for more details and additional bibliography.

The second lemma is a consequence of the previous one

Lemma 2 (Cf. Lemma 2.2 of [7])**.** *We have*

(a) *If* $F_n \mid m$, *then* $n \mid z(m)$.
(b) *If* $L_n \mid m$, *then* $2n \mid z(m)$.
(c) *If* $n \mid F_m$, *then* $z(n) \mid m$.

Lemma 3. *For all primes* $p \neq 5$, *we have that* $\gcd(z(p), p) = 1$.

Proof. By combining Lemma 1 (e) together with Lemma 2 (c), we conclude that $z(p) \mid p - (\frac{5}{p})$. Thus, when $p \neq 5$, one has that $(\frac{5}{p}) = \pm 1$ and so $z(p)$ divides $p-1$ or $p+1$. This yields that $z(p) = p+1$ or $z(p) \leq p-1$ and in any case $\gcd(z(p), p) = 1$. □

The next lemma will be very useful in the proof of our theorems. First, we recall the identities

$$\begin{aligned} F_a L_b &= F_{a+b} + (-1)^b F_{a-b}, \\ 5F_a F_b &= L_{a+b} - (-1)^b L_{a-b}, \\ L_a L_b &= L_{a+b} + (-1)^b L_{a-b} \end{aligned} \tag{2.1}$$

for all integers a and b. These identities can be easily deduced from Binet's formulas:

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ and } L_n = \alpha^n + \beta^n, \text{ for } n \geq 0,$$

where $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$.

Lemma 4. *Let* m *and* n *be positive integers, such that* $m \equiv n \pmod 4$. *Then*

(a) $F_{(m-n)/2} L_{(m+n)/2} = F_m - F_n$.
(b) $F_{(m+n)/2} L_{(m-n)/2} = F_m + F_n$.
(c) $L_{(m-n)/2} L_{(m+n)/2} = L_m + L_n$.
(d) $5F_{(m+n)/2} F_{(m-n)/2} = L_m - L_n$.

Proof. It suffices to use suitable choices of a and b in the identities (2.1). For example, if $a=(m-n)/2$ and $b=(m+n)/2$, then $a+b=m$ and $a-b=-n$. By (2.1), we have

$$F_{(m-n)/2}L_{(m+n)/2}=F_m+(-1)^{\frac{m+n}{2}+n+1}F_n,$$

where we used that $F_{-n}=(-1)^{n+1}F_n$. The proof of (a) is complete, since $(m+n)/2+n+1$ is odd. In fact, this follows from

$$m\equiv n \pmod 4 \Rightarrow \frac{m+n}{2}\equiv n \pmod 2 \Rightarrow \frac{m+n}{2}+n+1\equiv 2n+1 \pmod 2.$$

The other items can be proved in the same way. □

The p-adic order (or valuation) of r, $\nu_p(r)$, is the exponent of the highest power of a prime p which divides r. Throughout the paper, we shall use the known facts that $\nu_p(ab)=\nu_p(a)+\nu_p(b)$ and that $a \mid b$ if and only if $\nu_p(a)\le \nu_p(b)$, for all primes p.

We remark that the p-adic order of Fibonacci and Lucas numbers was completely characterized, see [2, 5, 12]. For instance, from the main results of Lengyel [5], we extract the following two results.

Lemma 5. *For $n\ge 1$, we have*

$$\nu_2(F_n)=\begin{cases} 0, & \text{if } n\equiv 1,2 \pmod 3;\\ 1, & \text{if } n\equiv 3 \pmod 6;\\ 3, & \text{if } n\equiv 6 \pmod{12};\\ \nu_2(n)+2, & \text{if } n\equiv 0 \pmod{12},\end{cases}$$

$\nu_5(F_n)=\nu_5(n)$, and if p is prime $\neq 2$ or 5, then

$$\nu_p(F_n)=\begin{cases} \nu_p(n)+\nu_p(F_{z(p)}), & \text{if } n\equiv 0 \pmod{z(p)};\\ 0, & \text{otherwise.}\end{cases}$$

Lemma 6. *Let $k(p)$ be the period modulo p of the Fibonacci sequence. For all primes $p\neq 5$, we have*

$$\nu_2(L_n)=\begin{cases} 0, & \text{if } n\equiv 1,2 \pmod 3;\\ 2, & \text{if } n\equiv 3 \pmod 6;\\ 1, & \text{if } n\equiv 0 \pmod 6\end{cases}$$

$$\nu_p(L_n)=\begin{cases} \nu_p(n)+\nu_p(F_{z(p)}), & \text{if } k(p)\neq 4z(p) \text{ and } n\equiv \frac{z(p)}{2} \pmod{z(p)};\\ 0, & \text{otherwise.}\end{cases}$$

With all of the above tools in hand, we now move to the proof of the theorem.

3. The proof of Theorem 1

3.1. *Item (i)*

By Lemma 4 (d), we have

$$L_m-L_n=5F_{\frac{m+n}{2}}F_{\frac{m-n}{2}}.$$

Since $F_{(m\pm n)/2}$ divides $L_m - L_n$, then $(m\pm n)/2 \mid z(L_m - L_n)$. Note that $(m-n)/2$ and $(m+n)/2$ are coprime which yields

$$\frac{m^2-n^2}{4} \mid z(L_m - L_n). \tag{3.1}$$

Also, $F_{(m\pm n)/2} \mid F_{(m^2-n^2)/4}$ and since

$$\gcd(F_{(m+n)/2}, F_{(m-n)/2}) = F_{\gcd((m+n)/2,(m-n)/2)} = F_1 = 1$$

we conclude that $F_{(m+n)/2}F_{(m-n)/2} \mid F_{(m^2-n^2)/4}$. Thus

$$L_m - L_n = 5F_{\frac{m+n}{2}}F_{\frac{m-n}{2}} \mid 5F_{\frac{m^2-n^2}{4}} \mid F_{5\left(\frac{m^2-n^2}{4}\right)},$$

where we used Lemma 1 (c). Therefore

$$z(L_m - L_n) \mid 5\cdot\left(\frac{m^2-n^2}{4}\right). \tag{3.2}$$

The combination between (3.1) and (3.2) yields

$$z(L_m - L_n) \in \left\{\frac{m^2-n^2}{4}, 5\cdot\left(\frac{m^2-n^2}{4}\right)\right\}.$$

Now, it suffices to prove that $5F_{(m+n)/2}F_{(m-n)/2} \nmid F_{(m^2-n^2)/4}$. In fact, this follows because

$$\begin{aligned}\nu_5(5F_{(m+n)/2}F_{(m-n)/2}) &= 1+\nu_5((m^2-n^2)/4)\\ &> \nu_5((m^2-n^2)/4) = \nu_5(F_{(m^2-n^2)/4}).\end{aligned}$$

This completes the proof. □

3.2. *Item (ii)*

Proceeding as before, we can easily deduce that

$$\frac{m^2-n^2}{4p} \mid z(L_m - L_n). \tag{3.3}$$

Here we used that $\gcd((m-n)/2,(m+n)/2) = p$ for all prime $p = \gcd(m,n)$.

Now, we claim that $L_m - L_n$ divides $F_{5F_p(m^2-n^2)/4p}$, or equivalently, that

$$\nu_q(5F_{(m+n)/2}F_{(m-n)/2}) \le \nu_q(F_{5F_p(m^2-n^2)/4p}),$$

holds for all primes q. Let us split the proof into four cases:

Case 1. $q = 5$. In this case, it follows directly that

$$\nu_5(5F_{(m+n)/2}F_{(m-n)/2}) = 1+\nu_5((m^2-n^2)/4)$$

while

$$\begin{aligned}\nu_5(F_{5F_p(m^2-n^2)/4p}) &= 1+\nu_5((m^2-n^2)/4)+\nu_5(F_p)-\nu_5(p)\\ &= 1+\nu_5((m^2-n^2)/4),\end{aligned}$$

where we used that $\nu_5(F_p) = \nu_5(p)$.

Case 2. $q = p \neq 2,5$. We have

$$\nu_p(5F_{(m+n)/2}F_{(m-n)/2}) = \nu_p((m+\delta n)/2) + \nu_p(F_{z(p)}),$$

where $\delta \in \{-1,1\}$ and we used that p cannot divide both $F_{(m+n)/2}$ and $F_{(m-n)/2}$, otherwise $z(p)$ would divide p which is an absurdity by Lemma 3. On the other hand, we have

$$\nu_p(F_{5F_p(m^2-n^2)/4p}) = \nu_p((m+\delta n)/2) + \nu_p((m-\delta n)/2) - 1 + \nu_p(F_{z(p)}).$$

The result follows because $\nu_p((m-\delta n)/2) \geq 1$, since $p = \gcd(m,n) > 2$.

Case 3. $q \neq 2,5,p$. In this case, we have

$$\nu_q(5F_{(m+n)/2}F_{(m-n)/2}) = \nu_q((m^2-n^2)/4) + \epsilon\nu_q(F_{z(q)}),$$

where ϵ is 1 or 2 according to the value of $\nu_q((m^2-n^2)/4)$ is 1 or not, respectively. For the other valuation, we obtain

$$\nu_q(F_{5F_p(m^2-n^2)/4p}) = \nu_q(F_p) + \nu_q((m^2-n^2)/4) + \nu_q(F_{z(q)}).$$

If $\epsilon = 1$, the conclusion is immediate. For $\epsilon = 2$, then $z(q) \mid p$ and so $z(q) = p$. Therefore $\nu_q(F_p) = \nu_q(F_{z(q)})$ and the result follows.

Case 4. $q = 2$. Since $\nu_2(5F_{(m+n)/2}F_{(m-n)/2}) = \nu_2(F_{(m+n)/2}) + \nu_2(F_{(m-n)/2})$, we need to consider two subcases:

Subcase 4.1 $p \neq 3$. In this case, 3 divides only one among $(m-n)/2$ and $(m+n)/2$. So, we have $\nu_2(5F_{(m+n)/2}F_{(m-n)/2}) = 1$, when $3 \mid (m+n)/2$ (because $(m+n)/2 \equiv 3 \pmod 6$) and when $3 \mid (m-n)/2$ one obtains $\nu_2(5F_{(m+n)/2}F_{(m-n)/2}) = 3$ or $\nu_2(m-n)+1$ depending on $(m-n)/4$ is odd or even, respectively. However, it is easy to infer that

$$\nu_2(F_{5F_p(m^2-n^2)/4p}) = \begin{cases} 1, & \text{if } 3 \mid (m+n)/2; \\ 3, & \text{if } 24 \nmid (m-n)/2; \\ \nu_2(m-n)+1, & \text{if } 24 \mid (m-n)/2, \end{cases}$$

yielding the desired inequality.

Subcase 4.2 $p = 3$. In this case, we get

$$\nu_2(5F_{(m+n)/2}F_{(m-n)/2}) = \begin{cases} 4, & \text{if } (m-n)/4 \text{ is odd}; \\ \nu_2(m-n)+2, & \text{if } (m-n)/4 \text{ is even}. \end{cases}$$

Now, note that $3 \mid m \pm n$ and $8 \mid (m^2-n^2)$ and then $12 \mid 5(m^2-n^2)/3$. Hence, by Lemma 5,

$$\nu_2(F_{5(m^2-n^2)/3}) = \nu_2((m^2-n^2)/3) + 2 = \nu_2(m-n) + 3 > \nu_2(m-n) + 2 \geq 4.$$

The result follows.

Summarizing, we proved that $L_m - L_n$ divides $F_{5F_p(m^2-n^2)/4p}$ and so, by Lemma 2 (c), we obtain

$$z(L_m - L_m) \mid 5F_p(m^2-n^2)/4p. \tag{3.4}$$

By (3.3) and (3.4), one concludes that

$$z(L_m - L_m) = t(m^2-n^2)/4p,$$

where t divides $5F_p$, that is, $5F_p = st$, for some positive integer s. Thus, in order to complete the proof of theorem, it suffices to prove that $s = 1$. Suppose, to derive a contradiction, that $s > 1$ and let q be a prime factor of s. Note that $q \neq p$ unless $p = 5$.

- $p = 5$ (and then $q = 5$). In this case, $25 = ts$ and so $t = 1, 5$ or 25. Note that

$$v_5(5F_{(m+n)/2}F_{(m-n)/2}) = 1 + v_5(m^2-n^2) > v_5(m^2-n^2) = v_5(F_{(m^2-n^2)/4}).$$

Thus $5F_{(m+n)/2}F_{(m-n)/2} \nmid F_{(m^2-n^2)/4}$ and the result follows.

- $p \neq 5$ (and so $q \neq 5$). Since $5F_p = ts$, then $q \mid F_p$ yielding $z(q) = p$. Therefore

$$v_q(5F_{(m+n)/2}F_{(m-n)/2}) = v_q((m+\delta n)/2) + 2v_q(F_{z(q)}),$$

where we used that q divides both $F_{(m+n)/2}$ and $F_{(m-n)/2}$, here $\delta \in \{0, 1\}$. On the other hand,

$$\begin{aligned} v_q(5F_{(m+n)/2}F_{(m-n)/2}) &= v_q(F_p) + v_q((m+\delta n)/2) - v_q(s) + v_q(F_{z(q)}) \\ &= v_q((m+\delta n)/2) - v_q(s) + 2v_q(F_{z(q)}) \\ &< v_q(5F_{(m+n)/2}F_{(m-n)/2}), \end{aligned}$$

since $q \mid s$ and we used that $v_q(F_p) = v_q(F_{z(q)})$. The proof of theorem is complete. □

4. Acknowledgements

The author thanks for support to Specific Research Project of Faculty of Science, University of Hradec Kralove, No. 2101, 2017.

References

[1] A. T. Benjamin and J. J. Quinn, "The Fibonacci numbers – exposed more discretely." *Math. Mag.*, vol. 76, no. 3, pp. 182–192, 2003, doi: 10.2307/3219319.

[2] J. Halton, "On the divisibility properties of Fibonacci numbers." *Fibonacci Q.*, vol. 4, pp. 217–240, 1966.

[3] D. Kalman and R. Mena, "The Fibonacci numbers – exposed." *Math. Mag.*, vol. 76, no. 3, pp. 167–181, 2003, doi: 10.2307/3219318.

[4] T. Koshy, *Fibonacci and Lucas numbers with applications.* New York, NY: Wiley, 2001.

[5] T. Lengyel, "The order of the Fibonacci and Lucas numbers." *Fibonacci Q.*, vol. 33, no. 3, pp. 234–239, 1995.

[6] F. Luca and C. Pomerance, "On the local behavior of the order of appearance in the Fibonacci sequence." *Int. J. Number Theory*, vol. 10, no. 4, pp. 915–933, 2014, doi: 10.1142/S1793042114500079.
[7] D. Marques, "On the order of appearance of integers at most one away from Fibonacci numbers," *Fibonacci Quart.*, vol. 50, no. 1, pp. 36–43, 2012, doi: 10.1155/2011/407643.
[8] D. Marques, "On integer numbers with locally smallest order of appearance in the Fibonacci sequence." *Int. J. Math. Math. Sci.*, vol. 2011, p. 4, 2011, doi: 10.1155/2011/407643.
[9] D. Marques, "The order of appearance of powers of Fibonacci and Lucas numbers." *Fibonacci Q.*, vol. 50, no. 3, pp. 239–245, 2012.
[10] D. Marques, "Sharper upper bounds for the order of appearance in the Fibonacci sequence." *Fibonacci Q.*, vol. 51, no. 3, pp. 233–238, 2013.
[11] P. Ribenboim, *My numbers, my friends. Popular lectures on number theory.* New York, NY: Springer, 2000. doi: 10.1007/b98892.
[12] D. Robinson, "The Fibonacci matrix modulo m." *Fibonacci Q.*, vol. 1, no. 2, pp. 29–36, 1963.
[13] H. Sallé, "A maximum value for the rank of apparition of integers in recursive sequences." *Fibonacci Q.*, vol. 13, pp. 159–161, 1975.
[14] N. J. A. Sloane, "The On-Line Encyclopedia of Integer Sequences." [Online]. Available: ttp://www.research.att.com/$\sim$njas/sequences/

Author's address

Pavel Trojovský
Faculty of Science University of Hradec Králové, Department of Mathematics, Rokitanského 62, Hradec Králové 50003, Czech Republic
E-mail address: pavel.trojovsky@uhk.cz