On the divisibility \( F_k \mid F_x^2 + F_x + 1 \)

Florian Luca\(^{a,d,e} \), Prapanpong Pongsriiam\(^{b,*} \), László Szalay\(^{c,f} \)

\(^{a}\) School of Maths, Wits University, Johannesburg, South Africa
\(^{b}\) Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000 Thailand
\(^{c}\) Department of Mathematics, J. Selye University, Komarno 94501 Slovakia
\(^{d}\) Research Group in Algebraic Structures and Applications, King Abdulaziz University, Jeddah 21589 Saudi Arabia
\(^{e}\) Centro de Ciencias Matemáticas, UNAM, Morelia 58089 Mexico
\(^{f}\) Institute of Mathematics, University of Sopron, Sopron 9400 Hungary

\(*\)Corresponding author, e-mail: pongsriiam_p@silpakorn.edu

Received 5 Jun 2020
Accepted 24 Nov 2020

ABSTRACT: Let \( F_n \) and \( L_n \) be the \( n \)th Fibonacci and Lucas numbers, respectively. We show that if \( F_k \mid F_x^2 + F_x + 1 \), then \( k \in \{4, 7\} \); if \( L_k \mid F_x^2 + F_x + 1 \), then \( k \in \{2, 4\} \).

KEYWORDS: Fibonacci number, Lucas number, divisibility, Diophantine equation, factorization

INTRODUCTION AND MAIN RESULTS

As usual, the sequence of Fibonacci numbers is defined by the recurrence \( F_n = F_{n-1} + F_{n-2} \) for \( n \geq 2 \) with the initial values \( F_0 = 0 \), \( F_1 = 1 \). This sequence can be extended for all integers \( n \) if one applies the recursive rule backward. This approach provides \( F_{-n} = (-1)^{n+1}F_n \) for all \( n \geq 0 \). The associated sequence of Lucas numbers is given by \( L_0 = 2 \), \( L_1 = 1 \), and \( L_n = L_{n-1} + L_{n-2} \) for \( n \geq 2 \). Its extension to \( Z \) satisfies \( L_{-n} = (-1)^nL_n \) for all \( n \geq 0 \). From a large number of identities involving Fibonacci numbers, we first recall

\[
F_a \equiv 1 = \begin{cases} 
F_{x+1}L_{x-1}, & \text{if } u \equiv 0 \pmod{4}; \\
F_{x+1}L_{x+1}, & \text{if } u \equiv 1 \pmod{4}; \\
F_{x+1}L_{x+2}, & \text{if } u \equiv 2 \pmod{4}; \\
F_{x+1}L_{x+3}, & \text{if } u \equiv 3 \pmod{4},
\end{cases} \tag{1}
\]

which provides a natural factorization of a Fibonacci number plus/minus 1. The verification of (1) can be done by using the well-known Binet formula and a straightforward calculation. Bravo, Komatsu, and Luca [1], and Luca and Szalay [3] used this formula in their calculations for the distance between the integers of the forms \( F_nF_{n+1} \cdots F_{n+k} \) and \( F_n^k \), and for the Fibonacci Diophantine tuples, respectively. Pongsriiam [7] also applied it in his solution to certain Diophantine equations, and a generalization of these equations is solved by Szalay [9]. Clearly, the equality \( F_u^2 - 1 = (F_u - 1)(F_u + 1) \) gives a kind of factorization into 4 factors, but after regrouping them, we obtain

\[
F_u^2 - 1 = \begin{cases} 
F_{u-2}F_{u+2}, & \text{if } u \equiv 0 \pmod{4}; \\
F_{u-1}F_{u+1}, & \text{if } u \equiv 1 \pmod{4}.
\end{cases} \tag{2}
\]

It is easy to see that there exists a similar formula for \( F_u^2 + 1 \) as follows:

\[
F_u^2 + 1 = \begin{cases} 
F_{u-1}F_{u+1}, & \text{if } u \equiv 0 \pmod{4}; \\
F_{u-2}F_{u+2}, & \text{if } u \equiv 1 \pmod{4}.
\end{cases} \tag{3}
\]

The formulas (2) and (3), and their generalizations are a tool in solving a variation of Brocard-Ramanajan equation as shown in the work of Pink and Szikszai [5], Pongsriiam [6], Sahukar and Panda [8], and Szalay [9]. Since \( F_u^3 - 1 = (F_u^2 - 1)(F_u^2 + 1) \), we obtain a factorization of \( F_u^3 - 1 \) from (2) and (3), but the question arises naturally: is there any Fibonacci or Lucas factorization of \( F_u^3 - 1 \)?

The identity \( F_u^3 - 1 = (F_u - 1)(F_u^2 + F_u + 1) \) shows that we need only to analyze the second factor.

It turned out that the situation is completely different from the other cases. The precise result is the following.

**Theorem 1** If \( k \geq 3 \) and \( F_k \mid F_n^2 + F_n + 1 \), then \( k = 4 \) (\( F_4 = 3 \)) or \( k = 7 \) (\( F_7 = 13 \)). Moreover

(i) \( 3 \mid F_x^2 + F_x + 1 \) if and only if \( x = 8t + 1 \) or \( x = 8t + 2 \) or \( x = 8t + 7 \) for some \( t \in \mathbb{Z} \);
We also investigated a related problem, where the divisor $F_k$ is replaced by the Lucas number $L_k$.

**Theorem 2** If $k \geq 2$ and $L_k \nmid F_x^2 + F_x + 1$, then $k = 2$ ($L_2 = 3$) or $k = 4$ ($L_4 = 7$). Moreover

(i) $3 \mid F_x^2 + F_x + 1$ if and only if $x = 8t + 1$ or $x = 8t + 2$ for some $t \in \mathbb{Z}$;

(ii) $7 \mid F_x^2 + F_x + 1$ if and only if $x = 16t + 3$ or $x = 16t + 12$ or $x = 16t + 13$ for some $t \in \mathbb{Z}$.

An easy consequence of the theorems above is

**Corollary 1** $F_x^2 + F_x + 1$ is never divisible by two distinct Lucas numbers larger than 1. In addition, $F_x^2 + F_x + 1$ is divisible by two distinct Fibonacci numbers larger than 1 if and only if $x = 56t + 10$ ($t \in \mathbb{Z}$), and in this case the two Fibonacci factors are 3 and 13.

To prove the main results, we recall the following two lemmas appearing in the proof of Theorem 1 of Németh, Soydan, and Szalay [4], and in Lemma 1 of Komatsu, Luca, and Tachiya [2].

**Lemma 1** (Németh, Soydan, and Szalay [4]) The sequence $(F_n)_{n \in \mathbb{Z}}$ is periodic modulo $F_k$ with period 4k.

**Lemma 2** (Komatsu, Luca, and Tachiya [2]) Let $X \geq 3$ be a real number. Let $a, b \in \mathbb{N}$ with $\max\{a, b\} \leq X$. Then there exist integers $u, v$ not both zero such that $\max\{|u|, |v|\} \leq \sqrt{X}$ and $|au + bv| \leq 3\sqrt{X}$.

**PROOF OF Theorem 1**

Assume that $F_k \mid F_x^2 + F_x + 1$. By Lemma 1, reducing $x$ modulo 4k in the relation $F_k \mid F_x^2 + F_x + 1$, we may assume that $|x| \leq 2k$. Now we write $\omega = e^{2\pi i/3}$ and $F_x^2 + F_x + 1 = (F_x - \omega)(F_x - \overline{\omega})$.

Writing $(\alpha, \beta) = ((1 + \sqrt{5})/2, (1 - \sqrt{5})/2)$, we have the Binet formula

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

valid for all $n \in \mathbb{Z}$.

Note that $\beta = -\alpha^{-1}$. Clearly

$$F_x - \omega = \frac{\alpha^x - \beta^x}{\sqrt{5}} - \omega = \frac{\alpha^x - (1)^x \alpha^{-x} - \sqrt{5}\omega}{\sqrt{5}} = \frac{\alpha^{-x}}{\sqrt{5}} \left(\alpha^x - \sqrt{5}\omega \alpha^x - (-1)^x\right),$$

and similarly

$$F_x - \overline{\omega} = \frac{\alpha^{-x}}{\sqrt{5}} \left(\alpha^x - \sqrt{5}\overline{\omega} \alpha^x - (-1)^x\right).$$

Thus,

$$F_k = \frac{(\alpha^x - \sqrt{5}\omega \alpha^x - (1)^x)}{\sqrt{5}} \cdot \frac{(\alpha^x - \sqrt{5}\overline{\omega} \alpha^x - (-1)^x)}{\sqrt{5}}.$$

The factors in the right-hand side are in the field $\mathbb{Q}(\omega, \sqrt{5}) \subset \mathbb{Q}(\zeta^{2n/15})$, which is a class number 1 field of degree 4. Thus, all ideals in $\mathfrak{O}_K$ are principal.

In fact, the two factors $F_x - \omega$ and $F_x - \overline{\omega}$ are almost coprime since their greatest common divisor divides $\omega - \overline{\omega} = i\sqrt{3}$ and $i\sqrt{3}$ is prime in $\mathfrak{O}_K$ since the prime 3 is inert in $\mathbb{Q}(\sqrt{5})$. Thus, these two factors are not coprime only if $F_x \equiv 1 \pmod{i\sqrt{3}}$ since otherwise $F_x^2 + F_x + 1$ is coprime to 3. Then

$$F_x - \omega \equiv 1 - \omega = \frac{3}{2} - \frac{\sqrt{3}}{2}i = -i\sqrt{3}\left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right) \equiv 0 \pmod{i\sqrt{3}}.$$ 

In this case $F_x^2 + F_x + 1 \equiv 3 \pmod{9}$, and the factor 3 gets split into two pieces associated to $i\sqrt{3}$ each, one which goes into $F_x - \omega$ and the other goes into $F_x - \overline{\omega}$, and the quotients remain coprime.

Hence, if $F_x \not\equiv 1 \pmod{3}$, or $F_x \equiv 1 \pmod{3}$ but $F_k$ is not a multiple of 3, then

$$F_k = \gcd\left(\frac{\alpha^x - \sqrt{5}\omega \alpha^x - (1)^x}{\sqrt{5}}\right) \times \gcd\left(\frac{\alpha^x - \sqrt{5}\overline{\omega} \alpha^x - (-1)^x}{\sqrt{5}}\right).$$

Otherwise, if $F_x \equiv 1 \pmod{3}$ and $3 \mid F_k$, then we divide across by 3 and get

$$F_k = \gcd\left(\frac{\alpha^x - \sqrt{5}\omega \alpha^x - (1)^x}{i\sqrt{15}}\right) \times \gcd\left(\frac{\alpha^x - \sqrt{5}\overline{\omega} \alpha^x - (-1)^x}{i\sqrt{15}}\right).$$

and now $(\alpha^x - \sqrt{5}\omega \alpha^x - (1)^x)/(i\sqrt{15})$ and $(\alpha^x - \sqrt{5}\overline{\omega} \alpha^x - (-1)^x)/(i\sqrt{15})$ are coprime.

To unify the two branches we introduce $\varepsilon = 1$ or $i\sqrt{3}$ according to the previous two cases. It follows that

$$\frac{F_k}{\varepsilon^2} \mathfrak{O}_K = \mathfrak{U} : \mathfrak{V} = (U \mathfrak{O}_K) : (V \mathfrak{O}_K),$$

(4)
Raising the first congruence in (6) to a and the second to b and multiplying them, we get
\[ a^{2ka+xb} - (-1)^ka_i z_i^b \equiv 0 \pmod{\mathcal{U}_i} \quad \text{for } i = 1, 2. \]

In particular,
\[ U \mathcal{O}_i \mid \mathcal{U}_i \mathcal{O}_i \mid (a^{2ka+xb} - (-1)^ka_i z_i^b)(a^{2kb} - (-1)^ka_i z_i^b). \]

The expression in the right hand side is symmetric in \( z_1, z_2 \) so it belongs to \( K \). Let us show that it is not zero. If it were, then
\[ a^{4ka+2xb} = z_i^{2b} \tag{7} \]
for some \( i = 1, 2 \). We checked that \( z_i \) is complex non real for both \( x \) even and odd. The same is true for \( \omega \) replaced by \( \omega^2 \). If \( b = 0 \), then \( a^{4ka} = 1 \), so \( a \) is false since we cannot have both \( a \) and \( b \) be zero. So, \( b \neq 0 \). We can now complex conjugate the above relation (7) to get that
\[ a^{4ka+2xb} = z_i^{2b}, \]
and taking ratios we get \( (z_i/\bar{z}_i)^{2b} = 1 \), so \( z_i/\bar{z}_i \) is a root of unity, and this is also false. In fact, it turns out that in all cases \( z_i/\bar{z}_i \) is of degree 4 and has two real conjugates, one of absolute value larger than 1 and one of absolute value smaller than 1 so it cannot be a root of unity. Thus, we get that
\[ U = v^{-1}(a^{2ka+xb} - (-1)^kz_i^b)(a^{2ka+kb} - (-1)^kz_i^b), \]
where \( v \) is some algebraic integer in \( K \). Thus,
\[ |U| = |v|^{-1} \left| (a^{2ka+xb} - (-1)^kz_i^b)(a^{2ka+kb} - (-1)^kz_i^b) \right|. \tag{8} \]
We computed the absolute values of \( z_i \) for \( i = 1, 2 \) and also of the analogous numbers with \( \omega \) replaced by \( \omega^2 \). We get that they are smaller than 2.5 < \( a^2 \). Thus,
\[ |a^{2ka+xb} - (-1)^kz_i^b| \leq a^{3\sqrt{2k}} + a^{2\sqrt{2k}} \]
\[ = a^{3\sqrt{2k}} \left( 1 + \frac{1}{a^{\sqrt{2k}}} \right). \]

Hence,
\[ |a^{2ka+xb} - (-1)^kz_i^b| \leq a^{\sqrt{2k}} \left( 1 + \frac{1}{a^{\sqrt{2k}}} \right)^2. \tag{9} \]

Doing this for \( \bar{U}, U^\sigma, U^\tau \) and using (5) as well as (8) and its conjugates and (9) and its conjugates, we get that
\[ F_k^2 \leq 9U\bar{U}U^\sigma U^\tau \leq 9|N_{K}\mathbb{Q}(\nu)|^{-1} \left( a^{\sqrt{2k}} \left( 1 + \frac{1}{a^{\sqrt{2k}}} \right)^2 \right)^4 \]
\[ \leq 9a^{24\sqrt{2k}} \left( 1 + \frac{1}{a^{\sqrt{2k}}} \right)^8. \tag{10} \]
Now
\[ P_k^2 = \frac{(a^k - \beta^k)^2}{5} \geq \frac{a^{2k}}{5} \left(1 - \frac{1}{\alpha^{2k}}\right)^2 \]
\[ \geq a^{2k-4} \left(1 + \frac{2}{\alpha^{2k}}\right)^2, \]
which together with (10), and 9 < \alpha^5 gives
\[ a^{2k-4} \leq a^{2\sqrt{2k} + 5} \left(1 + \frac{1}{\alpha^{2k}}\right)^8 \left(1 + \frac{2}{\alpha^{2k}}\right)^2. \]
For \( k \geq 300 \), the factor
\[ \left(1 + \frac{1}{\alpha^{2k}}\right)^8 \left(1 + \frac{2}{\alpha^{2k}}\right)^2 \]
is smaller than 1.00007. In particular, smaller than \( \alpha \). So,
\[ 2k < 24\sqrt{2k} + 10, \]
which gives \( \sqrt{2k} < 25 \), so \( k \leq 312 \). For \( k \in [3, 312] \) and \( x \in [0, 4k - 1] \), we checked \( F_k \mid F_{2k}^2 + F_x + 1 \), getting only the following values of \((k, x)\):
\[ (4, 1), (4, 2), (4, 7), (4, 9), (4, 10), (4, 15), (7, 4), (7, 10). \]
So, indeed \( k \in [4, 7] \). The rest of the statements come from the analysis of the sequence \((F_n^2 + F_n + 1)_{n \in \mathbb{Z}} \) modulo \( F_4 = 3 \) and modulo \( F_7 = 13 \), respectively.

**PROOF OF Theorem 2**

This proof is very similar to the proof of Theorem 1. Thus, we emphasize only the differences.

Assume that \( L_k \mid F_{2k}^2 + F_x + 1 \). First observe that since \( F_{2k} = F_k L_k \), we get that the sequence \( \{F_n\}_{n \geq 0} \) is periodic modulo \( L_k \) with period \( 8k \). Hence we suppose that \( |x| \leq 4k \). Clearly,
\[ L_k \left| \left(\frac{a^{2x} - \sqrt{5}\omega a^x - (-1)^x}{\sqrt{5}}\right) \cdot \left(\frac{a^{2x} - \sqrt{5}\omega a^x - (-1)^x}{\sqrt{5}}\right)\right.\]
and we have
\[ \frac{L_k}{\varepsilon^2} \partial_k \Psi = \Psi \cdot \Psi' = (U \partial_k) \cdot (V \partial_k). \]
(12)

Now
\[ \frac{L_k}{\varepsilon^2} = \lambda U \overline{U}, \]
and later
\[ U \partial_L \mid \Psi_1 \Psi_2, \]
where again \( \Psi_i = \gcd(\Psi \partial L, (\alpha^x - z_i) \partial L) \). In this case, the system of congruences is
\[ \alpha^{2k} \equiv (-1)^k \equiv (-1)^{k+1} \pmod{\Psi_1} \]
\[ \alpha^x \equiv z_i \pmod{\Psi_1}, \]
(13)
because \( \Psi_1 \mid \Psi \mid L_k \mid \alpha^k + \beta^k \) and
\[ \alpha^k + \beta^k = \alpha^{-k} (\alpha^{2k} + (-1)^k). \]
Knowing \( \max\{2k, |x|\} \leq 4k \), there are integers \( a, b \) with \( \max\{|a|, |b|\} \leq \sqrt{4k} = 2\sqrt{k} \) such that \( |2ka + \varepsilon b| \leq 6\sqrt{k} \). Subsequently,
\[ |\alpha^{2ka + \varepsilon b} - (-1)^{k+1} \bar{z}_i^b| \leq a^{6\sqrt{k}} + \alpha^{4k} \]
\[ = a^{6\sqrt{k}} \left(1 + \frac{1}{\alpha^{2\sqrt{k}}}\right). \]
Since \( L_k > F_k \), we get
\[ a^{2k-4} \leq a^{48\sqrt{k} + 5} \left(1 + \frac{1}{\alpha^{2\sqrt{k}}}\right)^8 \left(1 + \frac{2}{\alpha^{2k}}\right)^2, \]
and then
\[ 2k < 48\sqrt{k} + 10. \]
Hence \( k \leq 585 \). For \( k \in [2, 585] \) and \( x \in [0, 8k - 1] \), we checked \( L_k \mid F_{2k}^2 + F_x + 1 \), getting only the following values of \((k, x)\):
\[ (2, 1), (2, 2), (2, 7), (2, 9), (2, 10), (2, 15), (4, 3), (4, 12), (4, 13), (4, 19), (4, 28), (4, 29). \]
The rest of the statements come from the analysis of the sequence \( \{F_{2k}^2 + F_n + 1\}_{n \in \mathbb{Z}} \) modulo \( L_2 = 3 \) and modulo \( L_4 = 7 \), respectively.

**Acknowledgements:** F. L. is supported in part by Grant RTNUM2020 from the CoE MaSS of Wits. L. Sz. is supported by Hungarian National Foundation for Scientific Research Grant Nos. 128088 and 130909. This presentation has been made also in the frame of the “Erope-3.6.1-16-2016-00018 – Improving the role of the research + development + innovation in the higher education through institutional developments assisting intelligent specialization in Sopron and Szombathely”. P P is jointly supported by the Faculty of Science, Silpakorn University and the National Research Council of Thailand, Grant No. NRCT5–RSA63021–02.

**REFERENCES**