Arab Journal of Mathematical Sciences

Arab J Math Sci 24 (1) (2018) 9–15

On Fibonacci and Lucas sequences modulo a prime and primality testing

Dorin Andrica[a], Vlad Crişan[b,*], Fawzi Al-Thukair[c]

[a] Department of Mathematics, " Babeş-Bolyai" University, Cluj Napoca, Mihail Kogalniceanu Street 1, Cluj-Napoca, Romania
[b] Department of Mathematics, University of Göttingen, Bunsenstraße 3-5, Göttingen, Germany
[c] Department of Mathematics, College of Science, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia

Received 20 March 2017; accepted 20 June 2017
Available online 24 June 2017

Abstract. We prove two properties regarding the Fibonacci and Lucas Sequences modulo a prime and use these to generalize the well-known property $p \mid F_{p-\left(\frac{p}{5}\right)}$. We then discuss these results in the context of primality testing.

Keywords: Fibonacci and Lucas sequences; Legendre symbol

2010 Mathematics Subject Classification: 11A51; 11B39; 11B50

1. Introduction

The Fibonacci and Lucas sequences have been a topic of intensive investigation ever since they were introduced. Despite the huge amount of results that have been proved, they still present difficult and interesting problems which occupy the minds of mathematicians. In the

* Corresponding author.
E-mail addresses: dandrica@math.ubbcluj.ro (D. Andrica), vlad.crisan@mathematik.uni-goettingen.de (V. Crişan), thukair@ksu.edu.sa (F. Al-Thukair).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.ajmsc.2017.06.002

present article, we focus on discussing the properties of the two sequences when they are reduced modulo a prime.

Recall that the Fibonacci sequence $(F_n)_{n\geq 0}$ is defined by

$$F_0 = 0,\ F_1 = 1, \quad \text{and} \quad F_{n+1} = F_n + F_{n-1}, \quad \text{for} \quad n \geq 1,$$

while the Lucas sequence $(L_n)_{n\geq 0}$ is defined by:

$$L_0 = 2,\ L_1 = 1, \quad \text{and} \quad L_{n+1} = L_n + L_{n-1}, \quad \text{for} \quad n \geq 1.$$

The main result of the paper is Theorem 1, which generalizes the well-known property $p \mid F_{p-(\frac{p}{5})}$ to showing that $p \mid F_{kp-(\frac{p}{5})} - F_{k-1}$, where $\left(\frac{p}{5}\right)$ denotes the Legendre symbol. The equivalent result for the Lucas numbers is also derived as part of the same theorem. Results of similar flavor were previously derived in [8], Lemma 6 and in [7].

As a consequence of our main result, we generalize the notion of a Fibonacci pseudoprime and discuss its role in primality testing. This is achieved in Proposition 1 and in the remarks following it.

2. A key lemma

In this section we prove by elementary means an auxiliary lemma from which we will deduce our main result in the next section. Recall the Binet's formulas for F_n and L_n:

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right],$$

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

These formulas can be extended to negative integers n in a natural way. We have $F_{-n} = (-1)^{n-1}F_n$ and $L_{-n} = (-1)^n L_n$, for all n.

Our auxiliary result is the following:

Lemma 1. *Let p be an odd prime, k a positive integer, and r an arbitrary integer. The following relations hold:*

$$2F_{kp+r} \equiv \left(\frac{p}{5}\right) F_k L_r + F_r L_k \pmod{p} \tag{1}$$

and

$$2L_{kp+r} \equiv 5\left(\frac{p}{5}\right) F_k F_r + L_k L_r \pmod{p}, \tag{2}$$

where $(\frac{p}{5})$ is the Legendre's symbol.

Proof. We shall prove (1) directly from the definition. Write $(1+\sqrt{5})^s = a_s + b_s\sqrt{5}$, where a_s and b_s are positive integers, $s = 0, 1, \ldots$. By Binet's formula, we have

$$\begin{aligned} F_{kp+r} &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{kp+r} - \left(\frac{1-\sqrt{5}}{2}\right)^{kp+r}\right] \\ &= \frac{1}{2^{kp+r}\sqrt{5}}[(a_k + b_k\sqrt{5})^p(a_r + b_r\sqrt{5}) - (a_k - b_k\sqrt{5})^p(a_r - b_r\sqrt{5})] \end{aligned}$$

$$= \frac{1}{2^{kp+r}\sqrt{5}} \left[(a_r + b_r\sqrt{5}) \sum_{j=0}^{p} \binom{p}{j} a_k^{p-j} (b_k\sqrt{5})^j \right.$$
$$\left. -\ (a_r - b_r\sqrt{5}) \sum_{j=0}^{p} \binom{p}{j} (-1)^j a_k^{p-j} (b_k\sqrt{5})^j \right]$$
$$= \frac{1}{2^{kp+r}\sqrt{5}} \left[a_r \sum_{j=0}^{p} \binom{p}{j} (1-(-1)^j) a_k^{p-j} (b_k\sqrt{5})^j \right.$$
$$\left. +\ b_r\sqrt{5} \sum_{j=0}^{p} \binom{p}{j} (1+(-1)^j) a_k^{p-j} (b_k\sqrt{5})^j \right].$$

Since p divides $\binom{p}{j}$ for $j = 1, 2, \ldots, p-1$, it follows that

$$2^{kp+r-1} F_{kp+r} \equiv \left(a_r b_k^p 5^{\frac{p-1}{2}} + b_r a_k^p \right) \pmod{p}.$$

Using Fermat's Little Theorem and Euler's Criterion, we have further that

$$2^{kp+r-1} F_{kp+r} \equiv \left(\frac{p}{5}\right) a_r b_k + b_r a_k \pmod{p}, \tag{3}$$

where we have also used the Gauss' Quadratic Reciprocity Law to deduce that $(\frac{5}{p}) = (\frac{p}{5})$.

On the other hand, from $(1+\sqrt{5})^s = a_s + b_s\sqrt{5}$ we get $(1-\sqrt{5})^s = a_s - b_s\sqrt{5}$, hence we have $a_s = 2^{s-1} \cdot L_s$ and $b_s = 2^{s-1} \cdot F_s$ for $s = 0, 1, \ldots$. Substituting this back into (3), we obtain

$$2^{kp-k+1} F_{kp+r} \equiv \left(\frac{p}{5}\right) L_r F_k + F_r L_k \pmod{p},$$

and the relation (1) follows via Fermat's Little Theorem.

To deduce (2), we employ the following well-known formula:

$$L_n = F_n + 2F_{n-1},$$

which can be proved either directly from the definition or by noting that the sequences $(L_n)_{n\geq 0}$ and $(F_n + 2F_{n-1})_{n\geq 0}$ satisfy the same initial conditions and the same recursion formula. From this identity we can also immediately deduce that

$$L_n + 2L_{n-1} = 5F_n.$$

By (1), we have

$$2F_{kp+r} \equiv \left(\frac{p}{5}\right) F_k L_r + F_r L_k \pmod{p}$$

and

$$4F_{kp+r-1} \equiv 2\left(\frac{p}{5}\right) F_k L_{r-1} + 2F_{r-1} L_k \pmod{p}.$$

Adding these two relations yields

$$2F_{kp+r} + 4F_{kp+r-1} \equiv \left(\frac{p}{5}\right) F_k (L_r + L_{r-1}) + L_k (F_r + 2F_{r-1}).$$

Then using the two identities which we mentioned above we deduce that

$$2F_{kp+r} + 4F_{kp+r-1} = L_{kp+r}$$

and

$$\left(\frac{p}{5}\right) F_k(L_r + L_{r-1}) + L_k(F_r + 2F_{r-1}) = 5\left(\frac{p}{5}\right) F_k F_r + L_k L_r,$$

which gives the relation (2). □

3. The main result and primality testing

We begin by showing some immediate consequences of Lemma 1 and then derive the main result of this article, which generalizes the well-known property $p \mid F_{p-(\frac{p}{5})}$, which we also deduce below.

Examples 1. Taking $r = 0$ in relation (1), we obtain that for any positive integer k one has

$$F_{kp} \equiv \left(\frac{p}{5}\right) F_k \pmod{p}. \tag{4}$$

In the special case $k = 1$ we get

$$F_p \equiv \left(\frac{p}{5}\right) \pmod{p}.$$

Taking $k = 1$ and $r = 1$ in relation (1) we get

$$2F_{p+1} \equiv \left(\frac{p}{5}\right) + 1 \pmod{p}. \tag{5}$$

Taking $k = 1$ and $r = -1$ in relation (1) we get

$$2F_{p-1} \equiv -\left(\frac{p}{5}\right) + 1 \pmod{p}. \tag{6}$$

If $(\frac{p}{5}) = -1$, then from (5) we have $p \mid F_{p+1}$. In the case $(\frac{p}{5}) = 1$, from (6) one obtains $p \mid F_{p-1}$. We can summarize these consequences in the following known property:

$$p \mid F_{p-(\frac{p}{5})}. \tag{7}$$

Remark 1. We say that a composite number n is a **Fibonacci pseudoprime** if $n \mid F_{n-(\frac{n}{5})}$. Lehmer proved in [5] that there exist infinitely many such pseudoprimes. The list of the odd pseudoprimes is given in [1] A081264, while the list of the even ones is [1] A141137.

In contrast to (7), there is no prime $p < 2.8 \times 10^{16}$ such that $p^2 \mid F_{p-(\frac{p}{5})}$. R. Crandall, K. Dilcher and C. Pomerance called in [3] such a prime p satisfying $p^2 \mid F_{p-(\frac{p}{5})}$ a **Wall–Sun–Sun prime**. There is no known example of a Wall–Sun–Sun prime and there is also no known way to check the congruence $F_{p-(\frac{p}{5})} \equiv 0 \pmod{p^2}$, other than through explicit powering computations. Further remarks on this topic can be found in [2] or [4].

Examples 2. From relation (4), it follows that for two positive integers k and s, p divides $F_{kp} - F_{sp}$ if and only if p divides $F_k - F_s$. In particular, since $F_2 = F_1 = 1$, we get

$$p \mid F_{2p} - F_p.$$

Taking $k = 1$ and $r = 1$ in relation (2), we get

$$2L_{p+1} \equiv 5\left(\frac{p}{5}\right) + 1 \pmod{p}. \tag{8}$$

Taking $k = 1$ and $r = -1$ in relation (2) we get

$$2L_{p-1} \equiv 5\left(\frac{p}{5}\right) - 1 \pmod{p}. \tag{9}$$

If $(\frac{p}{5}) = -1$, then from (8) we have $p \mid L_{p+1} + 2$. In the case $(\frac{p}{5}) = 1$, from (9) one obtains $p \mid L_{p-1} - 2$.

We can summarize these remarks in the following formula:

$$p \mid L_{p-(\frac{p}{5})} - 2\left(\frac{p}{5}\right). \tag{10}$$

The relations (7) and (10) are just the first in a sequence of divisibility relations as we can see from the following result.

Theorem 1. *Let p be an odd prime and k a positive integer. The following relations hold :*

1. $F_{kp-(\frac{p}{5})} \equiv F_{k-1} \pmod{p}$.
2. $L_{kp-(\frac{p}{5})} \equiv (\frac{p}{5})L_{k-1} \pmod{p}$.

Proof. For the first part, let us consider in (1) $r = 1$ and $r = -1$ to get the relations $2F_{kp+1} \equiv (\frac{p}{5})F_k + L_k \pmod{p}$ and $2F_{kp-1} \equiv -(\frac{p}{5})F_k + L_k \pmod{p}$, respectively. These relations can be summarized as

$$2F_{kp-(\frac{p}{5})} \equiv L_k - F_k \pmod{p}.$$

The sequences $(L_j - F_j)_{j\geq 0}$ and $(2F_{j-1})_{j\geq 0}$ satisfy the same initial conditions for $j = 0$, $j = 1$ and the same recursive relation, hence we have $L_j - F_j = 2F_{j-1}$.

For the second part of the theorem, the argument is quite similar. Let us consider in (2) $r = 1$ and $r = -1$ to get the relations $2L_{kp+1} \equiv 5(\frac{p}{5})F_k + L_k \pmod{p}$ and $2L_{kp-1} \equiv 5(\frac{p}{5})F_k - L_k \pmod{p}$, respectively. These relations can be summarized as

$$2L_{kp-(\frac{p}{5})} \equiv \left(\frac{p}{5}\right)(5F_k - L_k) \pmod{p}.$$

Now observe that the sequences $(5F_j - L_j)_{j\geq 0}$ and $(2L_{j-1})_{j\geq 0}$ satisfy the same initial conditions for $j = 0$, $j = 1$ and the same recursive relation, hence we have $5F_j - L_j = 2L_{j-1}$, and the property is proved. □

Remark 2. The first relation in Theorem 1 shows that for every odd prime p, there exists an arithmetic progression $a_0, a_1, \ldots$ with ratio p, such that

$$(F_{a_0}, F_{a_1}, F_{a_2}, \ldots) \equiv (F_0, F_1, F_2, \ldots) \pmod{p}.$$

The second relation of the same theorem shows that for every odd prime p, there exists an arithmetic progression $a_0, a_1, \ldots$ with ratio p, such that

$$(L_{a_0}, L_{a_1}, L_{a_2}, \ldots) \equiv (L_0, L_1, L_2, \ldots) \pmod{p} \quad \text{if} \quad \left(\frac{p}{5}\right) = 1$$

and

$$(L_{a_0}, L_{a_1}, L_{a_2}, \ldots) \equiv -(L_0, L_1, L_2, \ldots) \pmod{p} \quad \text{if} \quad \left(\frac{p}{5}\right) = -1.$$

Following Theorem 1 we call a positive integer n a **Fibonacci pseudoprimes of level** k if n is composite and satisfies

$$n \mid F_{kn-\left(\frac{n}{5}\right)} - F_{k-1}.$$

This should not be confused with the well-known definition of a Fibonacci pseudoprime of kind k, which is connected to the generalized Lucas sequences.

For a fixed positive integer k, we denote by $\mathcal{F}_k$ the set of all Fibonacci pseudoprimes of level k. It is natural to ask whether the generalization provided by Theorem 1 gives better information about primality testing. Unfortunately, this is answered negatively by the following result:

Proposition 1. *Let $n > 0$ be an integer which is coprime to* 10*. Then $n \in \mathcal{F}_k$ for all $k \geq 1$ if and only if $n \in \mathcal{F}_1$ and $n \mid F_n^2 - 1$. In particular, if $n \mid F_{n-\left(\frac{n}{5}\right)}$ and $n \mid F_n - \left(\frac{n}{5}\right)$, then $n \in \mathcal{F}_k$ for all $k \geq 1$.*

Proof. Assume first that $n \in \mathcal{F}_1$ and $n \mid F_n^2 - 1$, i.e. n satisfies simultaneously $n \mid F_{n-\left(\frac{n}{5}\right)}$ and $n \mid F_n^2 - 1$. We prove by induction on $k \geq 1$ that $n \in \mathcal{F}_k$. This is true for $k = 1$ by our assumption. Recall Catalan's identity:

$$F_m^2 - F_{m+r}F_{m-r} = (-1)^{m-r}F_r^2.$$

We first use this for $m = n - \left(\frac{n}{5}\right)$ and $r = n$. As $5 \nmid n$, it follows that

$$F_{n-\left(\frac{n}{5}\right)}^2 + (-1)^{\left(\frac{n}{5}\right)}F_{2n-\left(\frac{n}{5}\right)} = (-1)^{-\left(\frac{n}{5}\right)}F_n^2.$$

Looking at this equality modulo n, we obtain that $n \mid F_{2n-\left(\frac{n}{5}\right)} - F_1$.

Assume now that the result holds for all positive integers less than some $k \geq 2$. To prove it for $k + 1$, we use Catalan's identity with $m = kn - \left(\frac{n}{5}\right)$, $r = n$ and we obtain

$$F_{kn-\left(\frac{n}{5}\right)}^2 - F_{(k+1)n-\left(\frac{n}{5}\right)}F_{(k-1)n-\left(\frac{n}{5}\right)} = (-1)^{(k-1)n-\left(\frac{n}{5}\right)}F_n^2.$$

Looking at this equality modulo n we obtain by the induction hypothesis that

$$F_{(k+1)n-\left(\frac{n}{5}\right)}F_{k-2} = F_{k-1}^2 - (-1)^{(k-1)n-\left(\frac{n}{5}\right)}.$$

Since $\gcd(n, 10) = 1$, we have that $(-1)^{(k-1)n-\left(\frac{n}{5}\right)} = (-1)^k$. On the other hand, applying Catalan's identity with $m = k$ and $r = 1$ we obtain

$$F_kF_{k-2} = F_{k-1}^2 + (-1)^{k-1}.$$

It follows that we must have $n \mid F_{(k+1)n-\left(\frac{n}{5}\right)} - F_k$, which completes the first part of our proof.

Conversely, if $n \in \mathcal{F}_k$ for all k, we have in particular that $n \in \mathcal{F}_1$ and $n \in \mathcal{F}_2$. Then from

$$F_{n-\left(\frac{n}{5}\right)}^2 + (-1)^{\left(\frac{n}{5}\right)}F_{2n-\left(\frac{n}{5}\right)} = (-1)^{-\left(\frac{n}{5}\right)}F_n^2$$

we deduce that $n \mid F_n^2 - 1$. $\square$

Remark 3. When $5 \mid n$ and n is odd, the above proof also shows that $n \in \mathcal{F}_k$ if and only if $n \mid F_{k-1}$. As $F_5 = 5$ and $\gcd(F_m, F_n) = F_{\gcd(m,n)}$, we get that $5 \mid k - 1$. As a particular case, using the identity

$$F_{5(2m+1)} = 5(F_{2m+1}^5 - 5F_{2m+1}^3 + F_{2m+1}),$$

one can easily prove by induction that $5^r \mid F_{5^r}$. Hence we obtain that $5^r \in \mathcal{F}_{k-1}$ whenever $5^r \mid k-1$.

Remark 4. Pseudoprimes n which satisfy the conditions $n \mid F_{n-\left(\frac{n}{5}\right)}$ and $n \mid F_n - \left(\frac{n}{5}\right)$ are discussed in [6], pages 126–129.

References

[1] http://oeis.org.

[2] V. Andrejic, On Fibonacci powers, Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. 17 (2006) 38–44.

[3] R. Crandall, K. Dilcher, C. Pomerance, A search for Wieferich and Wilson primes, Math. Comp. 66 (5) (1997) 433–449.

[4] J. Halton, Some properties associated with square Fibonacci numbers, Fibonacci Quart. (1967).

[5] E. Lehmer, On the infinitude of Fibonacci pseudoprimes, Fibonacci Quart. 2 (1964) 229–230.

[6] P. Ribenboim, The New Book of Prime Number Records, Springer, 1996.

[7] Gerhard Rosenberger, On some divisibility properties of Fibonacci and related numbers, Fibonacci Quart. (1983).

[8] B. Sury, Trigonometric expressions for Fibonacci and Lucas numbers, Acta Math. Univ. Comenian. 79 (2) (2010) 199–208.