ARAB JOURNAL OF
MATHEMATICAL SCIENCES

Arab J Math Sci ▮ (▮▮▮▮) ▮▮▮–▮▮▮

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 xxxx

Abstract. We prove two properties regarding the Fibonacci and Lucas Sequences modulo a prime and use these to generalize the well-known property $p \mid F_{p-(\frac{p}{5})}$. 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

Peer review under responsibility of King Saud University.
* 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.

ELSEVIER **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

$$F_{kp+r} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{kp+r} - \left(\frac{1-\sqrt{5}}{2}\right)^{kp+r}\right]$$

$$= \frac{1}{2^{kp+r}\sqrt{5}}[(a_k + b_k\sqrt{5})^p(a_r + b_r\sqrt{5}) - (a_k - b_k\sqrt{5})^p(a_r - b_r\sqrt{5})]$$

Please cite this article in press as: D. Andrica, et al., On Fibonacci and Lucas sequences modulo a prime and primality testing, Arab Journal of Mathematical Sciences (2017), http://dx.doi.org/10.1016/j.ajmsc.2017.06.002.