ON MODULI FOR WHICH THE LUCAS NUMBERS CONTAIN A COMPLETE RESIDUE SYSTEM

BRANDON AVILA AND YONGYI CHEN

Abstract. In 1971, Burr investigated the moduli for which the Fibonacci numbers contain a complete set of residues. In this paper, we examine the moduli for which this is true of the Lucas numbers.

1. Introduction

In 1971, Burr [2] proved the complete set of moduli m for which the Fibonacci numbers $(F_n)_{n=0}^{\infty}$ contain a complete set of residues to be all m taking the following forms:

$$5^k,\ 2 \cdot 5^k,\ 3^j \cdot 5^k,\ 4 \cdot 5^k,\ 6 \cdot 5^k,\ 7 \cdot 5^k,\ 14 \cdot 5^k \text{ for } k \geq 0,\ j \geq 1.$$

For example, the reduction of the Fibonacci numbers modulo 5 yields the sequence (0, 1, 1, 2, 3, 0, 3, 3, 1, 4, ...), where every residue is seen. But when reducing the sequence modulo 8, we find the repeating pattern $(0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, \ldots)$, which does not contain 4 or 6. The analogous set of moduli for Alcuin's Sequence was studied in 2012 by Bindner and Erickson [1].

The Lucas numbers $(L_n)_{n=0}^{\infty}$ are defined with the same recursion as the Fibonacci numbers ($L_n = L_{n-1} + L_{n-2}$), but with starting values $L_0 = 2$ and $L_1 = 1$. Here we explore the Lucas numbers, and those moduli for which the same property is seen. For the sake of brevity, we will call the moduli m for which the Fibonacci numbers and Lucas numbers contain all the residues mod m, *Fibonacci-complete* and *Lucas-complete*, respectively.

The theorem discussed in this paper was first conjectured by Erickson [3] in 2011.

2. Main Result

Theorem. *The Lucas-complete moduli are those of the following forms:*

$$2,\ 4,\ 6,\ 7,\ 14,\ 3^k \text{ for } k \geq 0.$$

First, we observe that the Lucas sequence modulo 5 is (2, 1, 3, 4, 2, 1, 3, 4, ...), in which no multiple of 5 appears. Thus it follows that if m is a multiple of 5, then m is not Lucas-complete. Also observe that if m is Lucas-complete, then $L_r \equiv 0 \pmod{m}$ for some r. We present the following lemmas.

Lemma 1. *If* $L_r \equiv 0 \pmod{m}$ *and* $L_{r+1} \equiv k \pmod{m}$, *then* $\gcd(m, k) = 1$.

Proof. Let $g = \gcd(m, k)$. Because g divides these two consecutive terms in the sequence, it follows by straightforward induction that g divides every term in the Lucas sequence. But $L_1 = 1$, so g divides 1, which implies that $g = 1$. □

Lemma 2. *If m is Fibonacci-complete and $L_r \equiv 0 \pmod{m}$ for some r, then m is Lucas-complete. If m is Lucas-complete, then m is Fibonacci-complete.*

Proof. For this proof, we will work in $\mathbb{Z}/m\mathbb{Z}$.

First, suppose that m is Fibonacci-complete and that $L_r = 0$, and let $k = L_{r+1}$. Then it follows by induction that $L_{r+n} = kF_n$ for all $n \geq 0$, that is, each term in the tail $(L_{n+r})_{n=0}^{\infty}$ is k times the corresponding term in $(F_n)_{n=0}^{\infty}$. In addition, we have $\gcd(m, k) = 1$ by Lemma 1. Therefore, if $(F_n)_{n=0}^{\infty}$ contains a complete residue system, then so does $(kF_n)_{n=0}^{\infty} = (L_{n+r})_{n=0}^{\infty}$. This proves the first statement.

Now suppose that $(L_n)_{n=0}^{\infty}$ contains a complete residue system. Then so does the tail $(L_{n+r})_{n=0}^{\infty}$, because $(L_n)_{n=0}^{\infty}$ is completely periodic. We now have that $(k^{-1}L_{n+r})_{n=0}^{\infty} = (F_n)_{n=0}^{\infty}$ also contains a complete residue system. This proves the second statement. □

At this point, it follows that if m is Lucas-complete, then m is of the form

$$2, 4, 6, 7, 14, 3^k \text{ for } k \geq 0.$$

It remains to show that all of the above moduli are indeed Lucas-complete. By Lemma 2, it suffices to show that there is a Lucas number divisible by m, for each of the above values of m.

It is easy to check that 1, 2, 4, 6, 7, and 14 have this property. We simply write out the sequences to show that $1 \mid L_0$, $2 \mid L_0$, $4 \mid L_3$, $6 \mid L_6$, $7 \mid L_4$, and $14 \mid L_{12}$. It remains to show that 3^k divides some Lucas number for all $k \geq 1$. We first make use of the following lemma.

Lemma 3. *If for some positive integer k, $3^k \mid L_n$, then $3^{k+1} \mid L_{3n}$.*

Proof. Making use of the identity $L_{3n} = L_n^3 - 3(-1)^n L_n$, we see that, since 3^{k+1} must divide L_n^3 (for positive k) and $3^{k+1} \mid 3(-1)^n L_n$ (that is, $3 \cdot 3^k \mid 3(-1)^n L_n$), 3^{k+1} divides a linear combination of the two, specifically, $L_n^3 - 3(-1)^n L_n = L_{3n}$. □

Since $3 \mid L_2 = 3$, by induction, 3^k divides some Lucas number for every positive integer k, and the theorem is proven.

3. Acknowledgement

We thank Dr. Martin Erickson for his support in reviewing and refining this paper to completion.

References

[1] D. Bindner and M. Erickson, *Alcuin's sequence*, American Mathematical Monthly, **119.2**, (2012), 115–121.
[2] S. A. Burr, *On moduli for which the Fibonacci sequence contains a complete system of residues*, The Fibonacci Quarterly, **9.5** (1971), 497–504.
[3] M. Erickson, *Beautiful Mathematics*, Mathematical Association of America, 2011, p. 132.

MSC2010: 11B50

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139
E-mail address: bavila@mit.edu

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139
E-mail address: yongyic@mit.edu