Ratio Mathematica Volume 41, 2021, pp. 71-78

Blocks within the period of Lucas sequence

Rima P. Patel*
Devbhadra V. Shah†

Abstract

In this paper, we consider the periodic nature of the sequence of Lucas numbers L_n defined by the recurrence relation $L_n = L_{n-1} + L_{n-2}$; for all $n \geq 2$; with initial condition $L_0 = 2$ and $L_1 = 1$. For any modulo $m > 1$, we introduce the 'blocks' within this sequence by observing the distribution of residues within a single period of Lucas sequence. We show that length of any one period of the Lucas sequence contains either $1, 2$ or 4 blocks.

Keywords: Fibonacci sequence, Lucas sequence, Periodicity of Lucas sequence

2010 AMS subject classification‡: 11B37, 11B39, 11B50

---

* Rima P. Patel (Mahavir Swami College of Polytechnic, Bhagwan Mahavir University, Surat, India); rimapatel25@gmail.com

†Devbhadra V. Shah (Department of Mathematics, Veer Narmad South Gujarat University, Surat, India); drdvshah@yahoo.com

‡ Received on September 21, 2021. Accepted on December 5, 2021. Published on December 31, 2021. doi: 10.23755/rm.v41i0.664. ISSN: 1592-7415. eISSN: 2282-8214.

1. Introduction

The Fibonacci sequence and the Lucas sequence are well-known sequences among all the integer sequences. The Fibonacci sequence $\{F_n\}$ satisfies the recurrence relation $F_n = F_{n-1} + F_{n-2}$, with the initial conditions $F_0 = 1$ and $F_1 = 1$. Lucas sequence $\{L_n\}$ is considered as the 'twin sequence' of Fibonacci sequence which satisfies the similar recursive relation $L_n = L_{n-1} + L_{n-2}$, with the initial conditions $L_0 = 2$ and $L_1 = 1$.

On the other hand, some researchers have conducted important research on the period of these two recursive sequences [1, 3, 4, 5, 6]. Wall [1] defines the length of period of the Fibonacci sequence by reducing it through the modulo any positive integer $m > 1$. Kramer and Hoggatt Jr. [3] also defined the length of the period of the Lucas sequence obtained by reducing the sequence through modulo any positive integer $m > 1$.

In this paper, we take deep insight in to the periodic nature of Lucas sequence and introduce the concept of 'blocks' by observing the distribution of residues within a single period of Lucas sequence when considered modulo any positive integer $m > 1$.

We denote the sequence of least non-negative residues of the terms of $\{L_n\}$ taken modulo m $(m \geq 2)$ by $L(mod\, m)$. If we examine the sequence of final digits of $\{L_n\}$, then we notice an interesting pattern that the sequence $L(mod\ 10) = \{2, 1, 3, 4, 7, 1, 8, 9, 7, 6, 3, 9, 2, 1, 3, ...\}$ repeats after the 12 terms again and again all the way. For any modulo m, it is easy to observe that the sequence $\{L_n\}$ is always periodic and it repeats from starting values 0 and 1. By $k_L = k_L(m)$, we mean the lengths of the period of $\{L_n\}$ modulo any positive integer m. These leads us to the following easy consequences.

Lemma 1.1. (a) $L_{k_L(m)-1} \equiv -1(modm)$ (b) $L_{k_L(m)} \equiv 2(modm)$
(c) $L_{k_L(m)+1} \equiv 1(modm)$ (d) $L_{k_L(m)+2} \equiv 3(modm)$
(e) $L_{k_L(m)+nr} \equiv L_n(mod\, m)$, for all $r \in \mathbb{Z}$.

The following is an important result which speaks about the divisibility property of $k_L(m)$.

Fact 1.2. For any $m > 1$, since $L(mod\, m)$ is always periodic, we conclude that if $L_n \equiv 2\ (mod\, m)$ and $L_{n+1} \equiv 1(mod\, m)$, then $k_L(m) \mid n$.

2. Blocks within $L(mod\ m)$

In this article, we restrict our attention to the behavior of the blocks within the residues for a given modulus and consequently some interesting relationships will be derived.

Definition 2.1. By $\alpha(m)$ we mean the smallest positive value of the index n of Lucas numbers such that $L_n \equiv 2L_{n+1}(mod\ m)$, when $n > 1$. We call $\alpha(m)$ the *restricted period* of $L(mod\ m)$.

Equivalently, $\alpha(m)$ is the position of the first repeated term in the sequence $L(mod\ m)$. Thus, $L_{\alpha(m)} \equiv 2L_{\alpha(m)+1}$ when considered $(mod\ m)$.

As an illustration, if we consider $L(mod\ 3) = \{2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1 ...\}$, then it is appearent that $L_4 \equiv 1(mod\ 3)$ and $L_5 \equiv 2(mod\ 3)$. Thus $L_4 \equiv 2L_5(mod\ 3)$, which gives $\alpha(3) = 4$.

We call the finite sequence $L_0,\ L_1, ... ,\ L_{\alpha(m)-1}$ to be the *first block* occurring in $L(mod\ m)$. It may happen that $\alpha(m) = k_L(m)$. In such case, we call $L(mod\ m)$ to be without restricted period.

For $L(mod\ 4) = \{2, 1, 3, 0, 3, 3, 2, 1, 3 ...\}$, clearly $\alpha(4) = k_L(4) = 6$, and thus $L(mod\ 4)$ has no restricted period.

Definition 2.2. By $s(m)$ we mean the second positive residue $'t'$, which appears after the first block in $L(mod\ m)$.

This clearly means that $2s(m) \equiv L_{\alpha(m)}\ (mod\ m)$; $s(m)\ = L_{\alpha(m)+1}$. Using the definition of L_n, we now conclude that $L_{\alpha(m)+2} = 3s(m)$, $L_{\alpha(m)+3} = 4s(m)$, $L_{\alpha(m)+4} = 7s(m), ...$. Also the first block ends with $m - s(m)$. Thus,

$$\left(L_{\alpha(m)},\ L_{\alpha(m)+1},\ L_{\alpha(m)+2},\ L_{\alpha(m)+3}, ...\right) = s(m)(2,\ 1,\ 3,\ 4,\ 7, ...)(mod\ m).$$

This implies that the successive terms in $L(mod\ m)$ after the first block are the multiples of $s(m)$. We therefore call $s(m)$ to be a *multiplier*.

Again, in the sequence $L(mod\ m)$, the blocks are of the form $2, 1, ..., m - s(m), 2s(m), s(m), ... ,\ m - x, x, x, ...$; where $2, 1, ..., m - s(m)$ is the first block, $2s(m), s(m), ..., m - x$ is the second block, and so on. The occurrence of $3 - 2m, m - 1$ in $L(mod\ m)$ will indicate that the end of the period has been reached and there after repetition begins, since the next two terms will be $2, 1$. Here we note that each block contains the same (that is $\alpha(m)$) number of terms and the subscripts are in arithmetic progression. Thus, $L_{\alpha(m)u} \equiv$

$2L_{\alpha(m)u+1}(mod\, m)$, for each positive integer u. Since $L_{k_L(m)} \equiv 2L_{k_L(m)+1}(mod\, m)$, we conclude that $\alpha(m)u = k_L(m)$, where u is a positive integer, which implies that $\alpha(m) \mid k_L(m)$. Later in the paper we show that the value of u is either 1 or 2 or 4.

Definition 2.3. By $\beta(m)$ we mean the order of $s(m)$, when considered modulo m. That is, $s(m)^{\beta(m)} \equiv 1\ (mod\, m)$ and if $n < \beta(m)$ then $s(m)^n \not\equiv 1\ (mod\, m)$.

To illustrate above definitions, we consider the following three examples:

(1) For $L(mod\ 4) = \{2, 1, 3, 0, 3, 3, 2, 1, \dots\}$, clearly $k_L(4) = 6$. Also, the restricted period $\alpha(4)$ is 6 and multiplier $s(4)$ is 1. Thus, the order of $s(4) = 1$ is 1 and hence $\beta(4) = 1$.

(2) If we consider $L(mod\ 6) = \{2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1, 0, 1, 1, 2, 3, 5, 2, 1, 3, 4, 1, \dots\}$, then clearly $k_L(6)$ is 24, $\alpha(6)$ is 12 and $s(m)$ is 5. Since $5^2 \equiv 1\ (mod\ 6)$, we get $\beta(11) = 2$.

(3) If we consider $L(mod\ 13) = 2, 1, 3, 4, 7, 11, 18, 3, 8, 11, 6, 4, 10, 1, 11, 12, 10, 9, 6, 2, 8, 10,\ 5, 2, 7, 9, 3, 12, 2, 1, 3, 4, \dots$, then $k_L(13) = 28$, $\alpha(13) = 7$ and $s(m) = 8$. Since $8^4 \equiv 1\ (mod\ 13)$, we have $\beta(13) = 4$.

The following theorem ties together the three functions $k_L(m)$, $\alpha(m)$ and $\beta(m)$.

Theorem 2.4. $k_L(m) = \alpha(m) \times \beta(m)$.

Proof: We first divide the single period of $L(mod\, m)$ into smaller finite subsequences, say $R_0, R_1, R_2, \dots, R_n, \dots$ as shown below:

$$\overbrace{2, 1, \dots\ 3s_1 - m, m - s_1}^{R_0}, \overbrace{2s_1, s_1, \dots, 3s_2 - m, m - s_2}^{R_1}, \overbrace{2s_2, s_2, \dots, 3s_3 - m, m - s_3}^{R_2} \dots$$

$$\dots \overbrace{2s_n, s_n, \dots, 3 - m, m - 1}^{R_n}, \overbrace{2, 1, \dots 3s_1 - m, m - s_1}^{R_{n+1}}, \dots, \qquad (2.1)$$

where $s_1 = s(m)$.

Obviously each finite subsequence 'R_i' has $\alpha(m)$ terms and it contains exactly one block. Hence every subsequence $R_i (i \geq 1)$ is a multiple of 'R_0'. Therefore, we have the following congruences modulo m:

$$R_1 = s_1 R_0\ ;\ R_2 = s_2 R_0\ ;\ R_3 = s_3 R_0\ ;\ \cdots\ ;\ R_{n-1} = s_{n-1} R_0\ ;\ R_n = s_n R_0.$$

Since the first term of R_1 is $m - s_2$ and that of R_0 is $m - s_1$ and we also have $R_1 = s_1 R_0$, we get $m - s_2 = s_1(m - s_1)$. If we consider the modulo m, we get $s_2 = s_1 \times s_1$. According to similar arguments, when considering the modulo

m, we have $s_3 = s_2 \times s_1, s_4 = s_3 \times s_1, s_5 = s_4 \times s_1, \cdots, s_n = s_{n-1} \times s_1$. Therefore, we have

$$\begin{aligned} s_n &= s_{n-1} \times s_1 \\ &= (s_{n-2} \times s_1) \times s_1 \\ &= (s_{n-3} \times s_1) \times s_1 \times s_1 \\ &\quad\vdots \\ &= \left(s_{n-(n-1)} \times s_1\right) \times \overbrace{s_1 \times s_1 \times \ldots \times s_1}^{(n-2)\ times} \end{aligned}$$

Thus, $s_n = s_1^n$.

Now since the order of s_1 is $\beta(m)$, we can write single period of $L(mod\ m)$ as follows:

$$2, 1, 3, 4, 7, \ldots, 3s_1 - m, m - s_1, s_1, \ldots, 3s_1^2 - m, m - s_1^2, s_1^2, \ldots, 3s_1^3 - m,$$
$$m - s_1^3, \ldots, 3 - m, m - 1, s_1^{\beta(m)-1}, \ldots, 2, 1.$$

Therefore, $\beta(m)$ can be interpreted differently as the number of blocks in a single period of $L(mod\ m)$. It now follows easily that $k_L(m) = \alpha(m) \times \beta(m)$.

Following are some interesting consequences which follows from these results.

Corollary 2.5. $L_{n\times\alpha(m)+r} \equiv \left(s(m)\right)^n \times L_r\ (mod\ m)$.
Proof: From the previous theorem, we have $R_n \equiv s_n R_0 (mod\ m)$ and $s_n \equiv s_1^n (mod\ m)$. Thus, we have

$$R_n \equiv s_1^n R_0\ (mod\ m). \tag{2.2}$$

This shows that the r^{th} term of R_n is equal to s_1^n times the r^{th} term of R_0, when considering the modulo m. Also, from the definition of $s(m)$, an immediate conclusion that would be drawn is $s_1 = 2L_{\alpha(m)}$ when considering modulo m. Therefore, from lemma 1.1 and above arguments, we can say that $L_{n\times\alpha(m)+r} \equiv \left(L_{\alpha(m)}\right)^n \times L_r\ (mod\ m)$. This finally gives $L_{n\times\alpha(m)+r} \equiv \left(s(m)\right)^n \times L_r\ (mod\ m)$.

Corollary 2.6. $gcd(m, s_i) = 1$; for all $i \geq 1$.
Proof: From the definition, when considered modulo m we have $s_n = s_1^n$. Therefore, we write ${s_i}^{\beta(m)} \equiv \left(s_1^i\right)^{\beta(m)} \equiv \left(s_1^{\beta(m)}\right)^i\ (mod\ m)$. Thus, since

$s_1^{\beta(m)} \equiv 1(mod\, m)$, we have $\left(s_1^{\beta(m)}\right)^i \equiv 1(mod\, m)$. This gives $s_i^{\beta(m)} \equiv 1(mod\, m)$. Now suppose $gcd(m, s_i) = d$. Then, $d \mid m$ and $d \mid s_i$, which gives $d \mid s_i^{\beta(m)}$. Also, $m \mid \left(s_i^{\beta(m)} - 1\right)$. Using both together, we have $d \mid \left(s_i^{\beta(m)} - \left(s_i^{\beta(m)} - 1\right)\right)$. This gives, $d = 1$. Thus, $gcd(m, s_i) = 1$.

Corollary 2.7. $s_n^r \equiv s_{n\times r}(mod\, m)$.
Proof: From the definition of $s(m)$, we have $s_n \equiv s_1^n(mod\, m)$. Then we can write $s_n^r \equiv (s_1^n)^r \equiv s_1^{n\times r} \equiv s_{n\times r}(mod\, m)$. It now follows that $s_n^r \equiv s_{n\times r}(mod\, m)$.

The following theorem doesn't seem to give us an immediate idea about $L(mod\, m)$, but some good results follow. The evidence comes from Robinson [2] but admits that Morgan Wood knew the result in the early 1930's.

Theorem 2.8. $k_L(m) = \gcd(2, \beta(m)) \times lcm[2, \alpha(m)]$, for $m > 2$.
Proof: Koshy [5] proved that $L_n^2 - L_{n-1}L_{n+1} = 5(-1)^n$. Taking $n = \alpha(m)$, we get

$$L_{\alpha(m)}^2 - L_{\alpha(m)-1}L_{\alpha(m)+1} = 5(-1)^{\alpha(m)}. \quad (2.3)$$

Now, $L_{\alpha(m)} \equiv 2s(m)(mod\, m)$, $L_{\alpha(m)-1} \equiv -s(m)(mod\, m)$ and $L_{\alpha(m)+1} \equiv s(m)(mod\, m)$. Therefore, by (2.2) we have

$$(2s(m))^2 - (-s(m))(s(m)) \equiv 5(-1)^{\alpha(m)}(mod\, m).$$

This gives

$$5(s(m))^2 \equiv 5(-1)^{\alpha(m)}(mod\, m). \quad (2.4)$$

Thus $\left(s(m)\right)^2$ and $(-1)^{\alpha(m)}$ has same order modulo m. But the order of -1 is 2 and the order of $s(m)$ is $\beta(m)$ modulo m. Thus,

$$\frac{\beta(m)}{\gcd(2,\beta(m))} = \frac{2}{\gcd(2,\alpha(m))}.$$

Thus,

$$k_L(m) = \alpha(m)\beta(m) = \alpha(m)\frac{2\gcd(2,\beta(m))}{\gcd(2,\alpha(m))} = \gcd(2, \beta(m)) \times lcm[2, \alpha(m)],$$

as required.

Finally, we calculate the possible values of $\beta(m)$.

Theorem 2.9. $\beta(m) = 1$ or 2 or 4; for any $m \geq 2$.
Proof: By above theorem we have

$$\mu(m) = \text{gcd}\big(2, \beta(m)\big) \times lcm[2, \alpha(m)], = (1\ or\ 2) \times \big(\alpha(m)\ or\ 2\alpha(m)\big).$$

Therefore, $\mu(m) = \alpha(m)$ or $2\alpha(m)$ or $4\alpha(m)$. Thus, we have $\beta(m) = 1$ or 2 or 4; for any $m \geq 2$.

We conclude the paper by noting the following obvious result which is a direct consequence of theorem 2.4 and theorem 2.9.

Corollary 2.10. $k(m) = \alpha(m)$ or $2\alpha(m)$ or $4\alpha(m)$.

3. Conclusion

In this article we had introduced the 'blocks' within the period of the Lucas sequence and shown that length of any one period of the Lucas sequence contains either $1, 2$ or 4 blocks.

References

[1] D. D. Wall. Fibonacci series modulo m. The American Mathematical Monthly, 67, 525 – 532, 1960.

[2] D. W. Robinson. The Fibonacci matrix modulo m. The Fibonacci Quarterly, 1, 29 – 36, 1963.

[3] J. Kramer, V. E. Jr. Hoggatt. Special cases of Fibonacci Periodicity. The Fibonacci Quarterly, 1:5, 519 – 522, 1972.

[4] K. Thomas. Fibonacci and Lucas Numbers with Applications. John Wiley and Sons,Inc., New York, 2001.

[5] R. Marc. Properties of the Fibonacci sequence under various moduli. Master's Thesis, Wake Forest University, 1996.

[6] R. P. Patel, D. V. Shah. Periodicity of generalized Lucas numbers and the length of its period under modulo 2^e. The Mathematics Today, 33, 67 – 74, 2017.