The Period of the Fibonacci Sequence Modulo j

Charles W. Campbell II
Math 399 Spring 2007
Advisor: Dr. Nick Rogers

Introduction

The main objectives of this project were to examine the Fibonacci sequence modulo j, a positive integer, with the intentions of generalizing the results to general sequences defined by linear recursions and to utilize information being acquired during the semester. The main part of the research involved investigating the periodicity of the new sequence obtained after modding out by j. We begin by establishing a motivation for investigating the sequence modulo p a prime and p^k a prime power by first investigating the Fibonacci sequence modulo j, a positive integer. Next we investigate the Fibonacci sequence modulo p a prime and then generalize to prime powers. True to the objective the results we obtained were through the use of (but not limited to) important ideas from both Number Theory and Abstract Algebra including Fermat's Little Theorem , Euler's generalization of Fermat's Little Theorem, Quadratic Reciprocity, and Field Theory. Lastly we apply the results established for the Fibonacci sequence to easily prove results for the Lucas sequence modulo p a prime.

We begin by defining the sequence itself.

Definition The *Fibonacci sequence* is a linear recursion defined by

$$F_{n+1} = F_{n-1} + F_n \qquad \text{for } n \geq 1, \tag{1}$$

where F_n is the nth Fibonacci number with $F_0 = 0$ and $F_1 = F_2 = 1$.

In the study of the Fibonacci sequence, it will be nice to be able to calculate the Fibonacci numbers themselves. There is a closed form equation for doing just that, but before we prove that this equation gives us the correct members of the sequence, we introduce the following identities which help us in the proof. Throughout let $\phi = \frac{1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$.

Identity 1.

$$\phi^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = \frac{2+1+\sqrt{5}}{2} = 1+\phi. \tag{2}$$

Identity 2.

$$\bar{\phi}^2 = \left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{1-2\sqrt{5}+5}{4} = \frac{6-2\sqrt{5}}{4} = \frac{3-\sqrt{5}}{2} = \frac{2+1-\sqrt{5}}{2} = 1+\bar{\phi}. \quad (3)$$

We are now prepared to state and prove the first and most widely used result, the closed form for generating the Fibonacci numbers.

Theorem 1. $F_n = \frac{1}{\sqrt{5}}(\phi^{\,n} - \bar{\phi}^{\,n})$.

Proof. Using induction on $n \in \mathbb{N}$ let P(n) be the statement that $F_n = \frac{1}{\sqrt{5}}(\phi^{\,n} - \bar{\phi}^{\,n})$. P(1) is true as

$$F_1 = \frac{1}{\sqrt{5}}(\phi - \bar{\phi}) = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}) = \frac{1+\sqrt{5}-1+\sqrt{5}}{2\sqrt{5}} = \frac{2\sqrt{5}}{2\sqrt{5}} = 1.$$

P(2) is true, since by (2) and (3) we have

$$F_2 = \frac{1}{\sqrt{5}}(\phi^{\,2} - \bar{\phi}^{\,2}) = \frac{1}{\sqrt{5}}((1+\phi) - (1+\bar{\phi})) = \frac{1}{\sqrt{5}}(\phi - \bar{\phi}) = F_1 = 1.$$

Now assume that P(n) is true up to some $n \in \mathbb{N}$, $n > 1$, and consider P($n+1$).

$$F_{n+1} = F_{n-1} + F_n = \frac{1}{\sqrt{5}}(\phi^{\,n-1} - \bar{\phi}^{\,n-1}) + \frac{1}{\sqrt{5}}(\phi^{\,n} - \bar{\phi}^{\,n})$$

$$= \frac{1}{\sqrt{5}}((\phi^{\,n-1} - \phi^{\,n}) - (\bar{\phi}^{\,n-1} - \bar{\phi}^{\,n}))$$

$$= \frac{1}{\sqrt{5}}(\phi^{\,n-1}(1+\phi) - \bar{\phi}^{\,n-1}(1+\bar{\phi}))$$

and by (2) and (3)

$$= \frac{1}{\sqrt{5}}(\phi^{\,n-1}(\phi^{\,2}) - \bar{\phi}^{\,n-1}(\bar{\phi}^{\,2})) = \frac{1}{\sqrt{5}}(\phi^{\,n+1} - \bar{\phi}^{\,n+1}).$$

Therefore P($n+1$) is true, so by induction, we conclude that P(n) is true $\forall\ n \in \mathbb{N}$. $\square$

Upon investigating the Fibonacci sequence modulo an integer j, it becomes evident that this modified sequence is periodic in nature. It should be noted that due to the nature of the recurrence relation defining F_n, from any point in the sequence, the future sequence is completely determined by two consecutive terms. Thus, considering two arbitrary consecutive members of the sequence modulo j, i.e the ordered pairs $(F_n \pmod j, F_{n+1} \pmod j)$, we see that there are j choices for each F_n and F_{n+1} so that there are j^2 possibilities for these consecutive numbers. Since there are a finite number of possibilities for these consecutive elements, our sequence must be eventually periodic, i.e. that it comes back to some member of the sequence and repeats thereafter. Again, due to the nature of the recurrence relation, we find that it is reversible, i.e. that we can go backwards in the sequence. Therefore we must come back to the beginning of the sequence, and thus we find that $F_n \pmod j$ must be purely periodic. Now that we know it exists, we are ready to define exactly what is meant by the period modulo j.

Definition The *period* of the Fibonacci sequence modulo a positive integer j is the smallest positive integer m such that $F_m \equiv 0 \pmod j$ and $F_{m+1} \equiv 1 \pmod j$.

Note that since $F_n \pmod j$ is purely periodic, if m is the period of $F_n \pmod j$, then every m-th member of the sequence modulo j must come back to the starting point. By the definition above, the only members that can possibly come back to the starting point are multiples of m. This can be summed up in the statement that if m is the period of $F_n \pmod j$, then for any $k \in \mathbb{Z}$

$$\begin{cases} F_k \equiv 0 \pmod j \\ F_{k+1} \equiv 1 \pmod j \end{cases} \quad \Leftrightarrow m \mid k. \tag{4}$$

The statement above and the corollary of the following theorem will be crucial in proving almost every theorem regarding the period modulo j.

Theorem 2. *Let p be a prime and let n be a positive integer. If $a \equiv 1 \pmod p$ then $a^{p^n} \equiv 1 \pmod{p^{n+1}}$.*

Proof. Suppose that $a \equiv 1 \pmod p$, and let $\mathrm{P}(n)$ be the statement that $a^{p^n} \equiv 1 \pmod{p^{n+1}}$. Since $a \equiv 1 \pmod p$, we know that $a = 1 + rp$ for some $r \in \mathbb{Z}$. Since $p^2 \mid (rp)^i$ for $2 \leq i \leq p$ we have that

$$a^p \equiv (1+rp)^p \equiv 1 + \binom{p}{1} rp + \sum_{i=2}^{p} \binom{p}{i} (rp)^i \equiv 1 + rp^2 + \sum_{i=2}^{p-1} \binom{p}{i} (rp)^i \equiv 1 \pmod{p^2}$$

Thus P(1) is true. Now assume that P(n) is true up to some n. So $a^{p^n} \equiv 1 \pmod{p^{n+1}}$ which implies that $a^{p^n} = 1 + sp^{n+1}$ for some $s \in \mathbb{Z}$. Now Consider P($n+1$).

$$a^{p^{n+1}} = (a^{p^n})^p = (1+sp^{n+1})^p = 1+\binom{p}{1}sp^{n+1}+\sum_{i=2}^{p}\binom{p}{i}(sp^{n+1})^i = 1+sp^{n+2}+\sum_{i=2}^{p}\binom{p}{i}(sp^{n+1})^i$$

and since $p^{n+2} \mid (sp^{n+1})^i$ for $2 \leq i \leq p$ we have that

$$a^{p^{n+1}} \equiv 1 + sp^{n+2} + \sum_{i=2}^{p}\binom{p}{i}(sp^{n+1})^i \equiv 1 \pmod{p^{n+2}}.$$

Therefore P(n) is true by induction. □

Corollary 1. *Let p be a prime and let k be a positive integer. If m is the period of F_n (mod p), then*

$$\phi^{mp^{k-1}} \equiv \bar{\phi}^{mp^{k-1}} \equiv 1 \ (mod\ p^k).$$

Proof. Since

$$F_m \equiv \frac{\phi^m - \bar{\phi}^m}{\sqrt{5}} \equiv 0 \pmod{p}$$

we have

$$\phi^m \equiv \bar{\phi}^m \pmod{p}.$$

$$F_m = F_{m+1} - F_1 = \frac{\phi^{m+1} - \bar{\phi}^{m+1}}{\sqrt{5}} - \frac{\phi - \bar{\phi}}{\sqrt{5}} = \frac{\phi^{m+1} - \bar{\phi}^{m+1} - \phi + \bar{\phi}}{\sqrt{5}} = \frac{\phi(\phi^m - 1) - \bar{\phi}(\bar{\phi}^m - 1)}{\sqrt{5}}.$$

Substituting ϕ^m for $\bar{\phi}^m$ we get

$$F_m \equiv \frac{\phi(\phi^m - 1) - \bar{\phi}(\bar{\phi}^m - 1)}{\sqrt{5}} \equiv \frac{\phi(\phi^m - 1) - \bar{\phi}(\phi^m - 1)}{\sqrt{5}} \equiv \frac{(\phi^m - 1)(\phi - \bar{\phi})}{\sqrt{5}}$$

$$\equiv (\phi^m - 1)F_1 \equiv (\phi^m - 1) \equiv 0 \pmod{p}.$$

Thus

$$\bar{\phi}^m \equiv \phi^m \equiv 1 \pmod{p},$$

so we can apply Theorem 2 to ϕ^m and $\bar{\phi}^m$ to conclude that

$$(\phi^m)^{p^{k-1}} \equiv (\bar{\phi}^m)^{p^{k-1}} \equiv 1 \pmod{p^k}.$$

□

We first investigate the period modulo a positive integer j in order to show that it is dependent on the period modulo the prime powers that divide j.

Theorem 3. *Let j be a positive integer with $j = \prod_{i=1}^{s} {p_i}^{k_i}$, for p_i a prime, and let m_i denote the period of $F_n \pmod{{p_i}^{k_i}}$. If m is the period of $F_n \pmod{j}$, then*

$$m = lcm(m_1, m_2, ..., m_s).$$

Proof. Let $j = \prod_{i=1}^{s} {p_i}^{k_i}$ be a positive integer, let m be the period of $F_n \pmod{j}$, and let m_i be the period of $F_n \pmod{{p_i}^{k_i}}$. So

$$\begin{cases} F_m \equiv 0 \pmod{j} \\ F_{m+1} \equiv 1 \pmod{j}. \end{cases}$$

Applying the Chinese Remainder Theorem to these congruences we have that

$$\begin{cases} F_{m_i} \equiv 0 \pmod{{p_i}^{k_i}} \\ F_{m_i+1} \equiv 1 \pmod{{p_i}^{k_i}} \end{cases} \qquad \forall i.$$

By (4) we also know that for $r \in \mathbb{Z}$

$$\begin{cases} F_{rm_i} \equiv 0 \pmod{{p_i}^{k_i}} \\ F_{rm_i+1} \equiv 1 \pmod{{p_i}^{k_i}} \end{cases} \qquad \forall i.$$

Letting $r = m_1 \cdots m_{i-1} \cdot m_{i+1} \cdots m_s$ we have that

$$m' = rm_i = \prod_{i=1}^{s} m_i$$

and

$$\begin{cases} F_{m'} \equiv 0 \pmod{\prod_{i=1}^{s} {p_i}^{k_i}} \\ F_{m'+1} \equiv 1 \pmod{\prod_{i=1}^{s} {p_i}^{k_i}} \end{cases} \qquad \forall i.$$

But this is not the period because $\text{lcm}(m_1, m_2, ..., m_s) = m^* \mid m'$, and by (4) we have that

$$\begin{cases} F_{m^*} \equiv 0 \pmod{\prod_{i=1}^{s} {p_i}^{k_i}} \\ F_{m^*+1} \equiv 1 \pmod{\prod_{i=1}^{s} {p_i}^{k_i}} \end{cases} \qquad \forall i.$$

Therefore since m^* is the least positive integer satisfying the above, by definition

$$m = m^* = \text{lcm}(m_1, m_2, ..., m_s).$$

□

Because the period modulo j depends on the prime powers dividing j, we are motivated to investigate the period modulo a prime power. To facilitate this, we need to look at the period modulo a prime p. In order to do this we must first determine the conditions under which we can apply Fermat's Little Theorem to ϕ, and $\bar{\phi}$. The following theorem determines the primes for which ϕ and $\bar{\phi}$ are elements of the field $\mathbb{Z}/p\mathbb{Z}$ which we denote $\mathbb{F}_p$.

Theorem 4. *Let $p \neq 5$ be a prime. Then 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod 5$, and 5 is a quadratic nonresidue modulo p if and only if $p \equiv \pm 2 \pmod 5$.*

Proof. Let p be a prime. Utilizing Quadratic Reciprocity we have

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\left(\frac{5-1}{2}\right)\left(\frac{p-1}{2}\right)} = \left(\frac{p}{5}\right)\left((-1)^{\frac{p-1}{2}}\right)^2 = \left(\frac{p}{5}\right)$$

$$\left(\frac{p}{5}\right) = \begin{cases} \left(\frac{1}{5}\right) = 1 & \Leftrightarrow\ p \equiv 1 \pmod 5 \\ \left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}} \equiv -1 \pmod 5 & \Leftrightarrow\ p \equiv 2 \pmod 5 \\ \left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} \equiv -1 \pmod 5 & \Leftrightarrow\ p \equiv 3 \pmod 5 \\ \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1 & \Leftrightarrow\ p \equiv 4 \pmod 5 \end{cases}$$

Therefore 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod 5$, and 5 is a quadratic nonresidue modulo p if and only if $p \equiv \pm 2 \pmod 5$. $\square$

By the above we conclude that for $p \equiv \pm 1 \pmod 5$, ϕ and $\bar{\phi}$ are elements of $\mathbb{F}_p$ and for $p \equiv \pm 2 \pmod 5$, ϕ and $\bar{\phi}$ are not elements of $\mathbb{F}_p$. In this second case we need to find an appropriate extension field of F_p that contains both ϕ and $\bar{\phi}$. The following theorems contain results regarding the period modulo p, a prime,

Theorem 5. *Let p be a prime and m be the period of $F_n \pmod p$. If $p \equiv \pm 1 \pmod 5$, then $m \mid p-1$.*

Proof. Let p be a prime, let m be the period of F_n modulo p, and suppose that $p \equiv \pm 1 \bmod 5$. Theorem 4 tells us that 5 is a quadratic residue for this choice of p, so we conclude that $\phi, \bar{\phi}$ are elements of $\mathbb{F}_p$. Applying Fermat's Little Theorem, we have

$$\phi^{p-1} \equiv 1 \pmod p \quad \text{and} \quad \bar{\phi}^{p-1} \equiv 1 \pmod p.$$

So

$$F_{p-1} \equiv \frac{1}{\sqrt{5}}\left(\phi^{p-1} - \bar{\phi}^{p-1}\right) \equiv \frac{1}{\sqrt{5}}(1-1) \equiv 0 \pmod p$$

and

$$F_p \equiv \frac{1}{\sqrt{5}}\left(\phi^{p} - \bar{\phi}^{p}\right) \equiv \frac{1}{\sqrt{5}}\left(\phi - \bar{\phi}\right) \pmod p$$

$$\equiv \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}-1+\sqrt{5}}{2}\right) \equiv \frac{1}{\sqrt{5}}\frac{2\sqrt{5}}{2} \pmod p$$

$$\equiv 1 \pmod p.$$

Therefore we have that

$$\begin{cases} F_{p-1} \equiv 0 \pmod p \\ F_p \equiv 1 \pmod p, \end{cases}$$

so by (4) we have that $m \big| p-1$. $\square$

Theorem 6. *Let p be a prime and m be the period of F_n (mod p). If $p \equiv \pm 2$ (mod 5), then $m \mid 2p+2$, with $\frac{2p+2}{m}$ odd.*

Proof. Let p be a prime, let m be the period of F_n mod p, and suppose that $p \equiv \pm 2 \bmod 5$. The Legendre symbol satisfies

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

For our choice of p and $a = 5$, Theorem 2 tells us that $5^{\frac{p-1}{2}} \pmod{p} \equiv -1$, and thus ϕ and $\bar{\phi}$ are not in $\mathbb{F}_p$. Therefore we work in the splitting field for $x^2 - 5$ over $\mathbb{F}_p$,

$$\mathbb{F}_p(\sqrt{5}) = \left\{ a + b\sqrt{5} \mid a, b \in \mathbb{F}_p \right\}.$$

Since this field has characteristic p and $5^{\frac{p-1}{2}} \pmod{p} \equiv -1$, we have

$$\begin{aligned}
\phi^p = \left(\frac{1+\sqrt{5}}{2}\right)^p &= \left(\frac{1}{2} + \frac{\sqrt{5}}{2}\right)^p = \left(\frac{1}{2}\right)^p + \left(\frac{\sqrt{5}}{2}\right)^p \\
&= \left(\frac{1}{2}\right)^p \left(1 + \sqrt{5}^p\right) = \frac{1}{2}\left(1 + 5^{\frac{p-1}{2}}\sqrt{5}\right) \\
&= \frac{1}{2}\left(1 - \sqrt{5}\right) = \frac{1-\sqrt{5}}{2} \\
&= \bar{\phi}.
\end{aligned}$$

Similarly

$$\begin{aligned}
\bar{\phi}^p = \left(\frac{1-\sqrt{5}}{2}\right)^p &= \left(\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^p = \left(\frac{1}{2}\right)^p - \left(\frac{\sqrt{5}}{2}\right)^p \\
&= \left(\frac{1}{2}\right)^p \left(1 - \sqrt{5}^p\right) = \frac{1}{2}\left(1 - 5^{\frac{p-1}{2}}\sqrt{5}\right) \\
&= \frac{1}{2}\left(1 + \sqrt{5}\right) = \frac{1+\sqrt{5}}{2} \\
&= \phi.
\end{aligned}$$

Therefore it is easily seen that

$$F_p \equiv \frac{\phi^p - \bar{\phi}^p}{\sqrt{5}} \equiv \frac{\bar{\phi} - \phi}{\sqrt{5}} \equiv (p-1) \pmod{p},$$

$$F_{p+1} \equiv \frac{\phi^{p+1} - \bar{\phi}^{p+1}}{\sqrt{5}} \equiv \frac{\phi^p\phi - \bar{\phi}^p\bar{\phi}}{\sqrt{5}} \equiv \frac{\bar{\phi}\phi - \phi\bar{\phi}}{\sqrt{5}} \equiv 0 \pmod{p},$$

and

$$F_{p+2} \equiv F_p + F_{p+1} \equiv (p-1) \pmod{p}$$

.

Therefore, for our choice of p, we see that m does not divide $p+1$. It is seen that

$$F_{2p+1} \equiv \frac{\phi^{2p+1} - \bar{\phi}^{2p+1}}{\sqrt{5}} \equiv \frac{\left(\phi^p\right)^2\phi - \left(\bar{\phi}^p\right)^2\bar{\phi}}{\sqrt{5}} \pmod{p}$$

$$\equiv \frac{\bar{\phi}^2\phi - \phi^2\bar{\phi}}{\sqrt{5}} \equiv \phi\bar{\phi}\left(\frac{\bar{\phi} - \phi}{\sqrt{5}}\right) \pmod{p}$$

$$\equiv (-1)\left(-F_1\right) \equiv (-1)(-1) \pmod{p}$$

$$\equiv 1 \bmod p,$$

$$F_{2p+2} \equiv \frac{\phi^{2p+2} - \bar{\phi}^{2p+2}}{\sqrt{5}} \equiv \frac{\left(\phi^p\right)^2\phi^2 - \left(\bar{\phi}^p\right)^2\bar{\phi}^2}{\sqrt{5}} \equiv \frac{\bar{\phi}^2\phi^2 - \phi^2\bar{\phi}^2}{\sqrt{5}} \equiv 0 \pmod{p},$$

and

$$F_{2p+3} \equiv F_{2p+1} + F_{2p+2} \equiv 1 \pmod{p}.$$

Therefore, since

$$\begin{cases} F_{2p+2} \equiv 0 \pmod{p} \\ F_{2p+3} \equiv 1 \pmod{p}, \end{cases}$$

by (4) we have that $m \Big| \ 2p+2$, and since m does not divide $p+1$, $\frac{2p+2}{m}$ must be odd. $\square$

Now that we have results regarding the period of $F_n \pmod{p}$ we are ready to investigate the period modulo a prime power, i.e. the period of $F_n \pmod{p^k}$.

Theorem 7. *Let p be a prime, let m denote the period of F_n modulo p, and let m' denote the period of F_n modulo p^k. Then $m' \mid mp^{k-1}$.*

Proof. By Corollary 1 we know that

$$\phi^{mp^{k-1}} \equiv \bar{\phi}^{mp^{k-1}} \equiv 1 \pmod{p^k}.$$

Therefore

$$F_{mp^{k-1}} \equiv \frac{\phi^{mp^{k-1}} - \bar{\phi}^{mp^{k-1}}}{\sqrt{5}} \equiv \frac{1-1}{\sqrt{5}} \equiv 0 \pmod{p^k}$$

and

$$F_{mp^{k-1}+1} \equiv \frac{\phi^{mp^{k-1}+1} - \bar{\phi}^{mp^{k-1}+1}}{\sqrt{5}} \equiv \frac{(\phi^{mp^{k-1}})\phi - (\bar{\phi}^{mp^{k-1}})\bar{\phi}}{\sqrt{5}} \equiv \frac{\phi - \bar{\phi}}{\sqrt{5}} \equiv 1 \pmod{p^k}$$

Therefore by (4) we have that $m' \mid mp^{k-1}$. □

In every known case of the above theorem $m' = mp^{k-1}$, but there are thought to be infinitely many primes for which this is not true. Since we now have results regarding the period of $F_n \pmod{p^k}$ we can apply Theorem 3 to tell us about the period modulo the product of prime powers. Therefore given a positive integer j we can determine the possibilities for the period of $F_n \pmod{j}$. That is, given j a positive integer and m the period modulo j, we can apply Theorems 3, 5, 6, and 7 to tell us that m divides a certain number t, but we can't be certain if t equals m or not.

We now turn our attention to another sequence defined by a recursion relation that is closely related to the Fibonacci sequence, the Lucas sequence.

Definition The *Lucas sequence* is a linear recursion defined by

$$L_{n+1} = L_{n-1} + L_n, \quad \text{for } n \geq 1,$$

where L_n is the nth Lucas number with $L_0 = 2$ and $L_1 = 1$.

Like the Fibonacci numbers, there is a closed form equation that makes calculating the Lucas numbers easier.

Theorem 8. $L_n = \left(\phi^n + \bar{\phi}^n\right)$

Proof. Using induction, let P(n) be the statement $L_n = \left(\phi^n + \bar{\phi}^n\right)$. P(0) is true since

$$L_0 = \phi^0 + \bar{\phi}^0 = 1 + 1 = 2$$

and P(1) is true as

$$L_1 = \phi + \bar{\phi} = \frac{1 + \sqrt{5} + 1 - \sqrt{5}}{2} = \frac{2}{2} = 1.$$

Now assume that P(n) is true for some $n \in \mathbb{N}$ and consider P($n+1$).

$$\begin{aligned} L_{n+1} = \phi^{n+1} + \bar{\phi}^{n+1} &= \phi^{n-1}\left(\phi^2\right) + \bar{\phi}^{n-1}\left(\bar{\phi}^2\right) \\ &= \phi^{n-1}\left(1 + \phi\right) + \bar{\phi}^{n-1}\left(1 + \bar{\phi}\right) \\ &= \phi^{n-1} + \phi^n + \bar{\phi}^{n-1} + \bar{\phi}^n \\ &= \left(\phi^{n-1} + \bar{\phi}^{n-1}\right) + \left(\phi^n + \bar{\phi}^n\right) \\ &= L_{n-1} + L_n \end{aligned}$$

Therefore P(n) is true for all n. □

Like the Fibonacci sequence, when we investigate the Lucas sequence modulo j an integer, we find that the new sequence is purely periodic and for the same reasons as Fibonacci sequence.

Definition The *period* of the Lucas sequence modulo a positive integer j is the smallest positive integer l such that $L_l \equiv 2 \pmod{j}$ and $L_{l+1} \equiv 1 \pmod{j}$.

Again, for the same reasons as the Fibonacci sequence we have that if l is the period of $L_n \pmod{j}$ then

$$\begin{cases} L_k \equiv 2 \pmod{j} \\ L_{k+1} \equiv 1 \pmod{j} \end{cases} \Leftrightarrow l \mid k \tag{5}$$

Theorem 9. *For p be a prime, let l be the period of L_n (mod p). If $p \equiv \pm 1 (mod\ 5)$, then $l \mid p - 1$.*

Proof. Let p be a prime, let l be the period of $L_n \bmod p$ and suppose that $p \equiv \pm 1 \pmod 5$. Since $p \equiv \pm 1 \pmod 5$ we know that $\phi, \bar{\phi} \in \mathbb{F}_p$ and thus

$$L_{p-1} \equiv \phi^{p-1} + \bar{\phi}^{p-1} \equiv 1 + 1 \bmod p \equiv 2 \pmod p$$

and

$$L_p \equiv \phi^p + \bar{\phi}^p \equiv \phi + \bar{\phi} \equiv \frac{1+\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2} = \frac{2}{2} \equiv 1 \pmod p.$$

Therefore by (5) we have that $l \mid p - 1$.

□

Theorem 10. *For p be a prime, let l be the period of $L_n \pmod p$. If $p \equiv \pm 2 \pmod 5$, then $l \mid 2p + 2$.*

Proof. Let p be a prime, let l be the period of $L_n \pmod p$ and suppose that $p \equiv \pm 2 \pmod 5$. Since $p \equiv \pm 2 \pmod 5$ we know that $\phi^p \equiv \bar{\phi} \pmod p$ and $\bar{\phi}^p \equiv \phi \pmod p$. Thus we have

$$L_{2p+2} \equiv \phi^{2p+2} + \bar{\phi}^{2p+2} \equiv (\phi^p)^2\phi^2 + (\bar{\phi}^p)^2\bar{\phi}^2 \pmod p$$

$$\equiv \bar{\phi}^2\phi^2 + \phi^2\bar{\phi}^2 \equiv 2(\phi\bar{\phi})^2 \equiv 2(-1)^2 \pmod p$$

$$\equiv 2 \pmod p$$

and

$$L_{2p+3} \equiv \phi^{2p+3} + \bar{\phi}^{2p+3} \equiv (\phi^p)^2\phi^3 + (\bar{\phi}^p)^2\bar{\phi}^3 \pmod p$$

$$\equiv \bar{\phi}^2\phi^3 + \phi^2\bar{\phi}^3 \equiv (\phi\bar{\phi})^2(\phi + \bar{\phi}) \equiv (-1)^2(1) \pmod p$$

$$\equiv 1 \pmod p.$$

Therefore by (5) we have that $l \mid 2p + 2$. □

References

[1] Gallian, Joe A. *Contemporary Abstract Algebra. Sixth Edition.* Houghton Mifflin. 2006.

[2] Niven, Zuckerman, Montegomery. *An Introduction to the Theory of Numbers. Fifth Edition.* John Wiley Sons, Inc. 1991.