Abstract

Let $F_n$ and $L_n$ denote the Fibonacci and Lucas sequences, respectively. We will study when a prime $p \equiv 1 \pmod{4}$ divides $L_{(p-1)/4}$ or $F_{(p-1)/4}$.

1. Introduction and Main Result

We begin our discussion with the definition of Lucas sequences.

**Definition 1.** Let $P$ and $Q$ be relatively prime integers. The Lucas sequences are defined by $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$ and

$$U_n = PU_{n-1} - QU_{n-2} \quad \text{and} \quad V_n = PV_{n-1} - QV_{n-2},$$

where $n \geq 2$. Also, let $\Delta = P^2 - 4Q$.

The Fibonacci and Lucas numbers, $F_n$ and $L_n$, are special cases of the $U$ and $V$ sequences when $P = 1$ and $Q = -1$. The following theorem was partially known to Lucas in 1878 and completely known to Lehmer in 1930. The proof of this theorem can be found in [2, p. 85].

**Theorem 2.** Let $p$ be an odd prime and assume $p$ is relatively prime to $Q$ and $\Delta$. Let $\epsilon = (\Delta/p)$, where $(\Delta/p)$ denotes the Jacobi symbol. Then

$$p|V_{(p-\epsilon)/2}, \quad \text{if } (Q/p) = -1$$

and

$$p|U_{(p-\epsilon)/2}, \quad \text{if } (Q/p) = 1.$$
Our main result follows. The statement of the theorem and its proof are similar in nature to a problem and solution in *The Fibonacci Quarterly* [1].

**Theorem 3.** Let $p$ be an odd prime and $i = \sqrt{-1}$.

(a) If $p \equiv 1 \pmod{40}$ or $p \equiv 9 \pmod{40}$, then

\[
p | L_{(p-1)/4} \quad \text{if and only if} \quad (1+2i)^{(p-1)/2}(2-i)+(1-2i)^{(p-1)/2}(2+i) \equiv 4 \pmod{p}
\]

and

\[
p | F_{(p-1)/4} \quad \text{if and only if} \quad (1+2i)^{(p-1)/2}(2-i)+(1-2i)^{(p-1)/2}(2+i) \not\equiv -4 \pmod{p}.
\]

(b) If $p \equiv 21 \pmod{40}$ or $p \equiv 29 \pmod{40}$, then

\[
p | L_{(p-1)/4} \quad \text{if and only if} \quad (1+2i)^{(p-1)/2}(2-i)+(1-2i)^{(p-1)/2}(2+i) \equiv 4 \pmod{p}
\]

and

\[
p | F_{(p-1)/4} \quad \text{if and only if} \quad (1+2i)^{(p-1)/2}(2-i)+(1-2i)^{(p-1)/2}(2+i) \not\equiv 4 \pmod{p}.
\]

2. **Proof of the Main Result**

Before we can prove our main result we need the following lemma.

**Lemma 4.** Let $\theta = \tan^{-1} 2$ and

\[
\cos j\theta = \frac{c_j}{5^{j/2}}.
\]

Then for $n \geq 0$,

\[
2^{2n-1}L_n = \sum_{k=0}^{n} \binom{2n}{2k} 5^{(n-|n-2k|)/2} c_{n-2k}.
\]

**Proof.** Consider the Lucas polynomials defined by $L_0(x) = 2$, $L_1(x) = x$, and $L_{n+2}(x) = xL_{n+1}(x) + L_n(x)$ for $n \geq 0$. It is well-known that

\[
L_n(x) = \left(\frac{x + \sqrt{x^2 + 4}}{2}\right)^n + \left(\frac{x - \sqrt{x^2 + 4}}{2}\right)^n, \quad n \geq 0.
\]
Note that $L_n = L_n(1)$, for $n \geq 0$. Next, we define

$$
\sin j\theta = \frac{s_j}{5|j|/2}.
$$

If $t \neq 1$ is any complex number, then

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

Applying the binomial theorem we obtain

$$
L_n \left( \frac{2i}{1-t} \right) = \frac{2i^n}{(1-t)^n} \sum_{k=0}^{n} \binom{2n}{2k} t^k.
$$

Now we take $t = (-3 - 4i)/5$. Then,

$$
\frac{2i}{1 - (-3 - 4i)/5} = 1 \quad \text{and} \quad \frac{1}{1 - (-3 - 4i)/5} = \frac{8 + 4i}{5}.
$$

Therefore by some algebra, we have

$$
L_n = L_n(1) = \frac{2i^n}{(\frac{8+4i}{5})^n} \sum_{k=0}^{n} \binom{2n}{2k} \left( \frac{-3 - 4i}{5} \right)^k
$$

$$
= 2^{1-2n} \sum_{k=0}^{n} \binom{2n}{2k} (1 + 2i)^n \left( \frac{-3 - 4i}{5} \right)^k (1 + 2i)^k
$$

$$
= 2^{1-2n} \sum_{k=0}^{n} \binom{2n}{2k} (1 + 2i)^{n-k} \left( \frac{5 - 10i}{5} \right)^k (1 - 2i)^k
$$

Now, since $\theta = \tan^{-1} 2$ we have

$$
1 \pm 2i = \sqrt{5}e^{\pm i\theta}.
$$
Continuing to simplify the above expression, we have

\[ L_n = 2^{1-2n} \sum_{k=0}^{n} \binom{2n}{2k} (\sqrt{5})^{n-k} e^{i(n-k)\theta} (\sqrt{5})^k e^{-ik\theta} \]

\[ = 2^{1-2n} \sum_{k=0}^{n} \binom{2n}{2k} 5^{n/2} e^{i(n-2k)\theta}. \]

Using the fact that the values of \( L_n \) are integers we have that

\[ 2^{2n-1} L_n = \sum_{k=0}^{n} \binom{2n}{2k} 5^{n/2} e^{i(n-2k)\theta} \]

\[ = \sum_{k=0}^{n} \binom{2n}{2k} 5^{n/2} 5^{-(|n-2k|)/2} c_{n-2k} \]

\[ = \sum_{k=0}^{n} \binom{2n}{2k} 5^{(n-|n-2k|)/2} c_{n-2k}. \]

This completes the proof of Lemma 4.

Now we need another lemma.

**Lemma 5.** Let \( p \) be a prime such that \( p \equiv 1 \pmod{4} \). Then,

\[ 2^{p-2} L_{\frac{p-1}{2}} \equiv \frac{1}{4} \left( (1 + 2i)^{(p-1)/2} (2 - i) + (1 - 2i)^{(p-1)/2} (2 + i) \right) \pmod{p}. \]

**Proof.** Let \( \theta = \tan^{-1} 2 \) and

\[ \cos j\theta = \frac{c_j}{5^{j/2}} \quad \text{and} \quad \sin j\theta = \frac{s_j}{5^{j/2}}. \]

Using Lemma 4 with \( n = (p - 1)/2 \) and the fact that if \( p \) is an odd prime, then

\[ \binom{p-1}{k} \equiv (-1)^k \pmod{p}, \quad \text{for} \quad k = 1, 2, \ldots, k - 1 \]

we have that

\[ 2^{p-2} L_{\frac{p-1}{2}} = \sum_{k=0}^{(p-1)/2} \binom{p-1}{2k} 5^{\frac{p-1}{2} - 2k} c_{\frac{p-1}{2} - 2k} \]

\[ \equiv \sum_{k=0}^{(p-1)/2} 5^{\frac{p-1}{2} - 2k} c_{\frac{p-1}{2} - 2k} \pmod{p}. \]
Simplifying the above expression using properties of the sin, cos, and exp functions, the sum of a geometric series, the definition of \( c_j \) and \( s_j \), and complex arithmetic we have

\[
\sum_{k=0}^{(p-1)/2} 5 \frac{\frac{p-1}{2} - \frac{p-1}{2} - 2k}{c_{\frac{p-1}{2} - 2k}} = \left( \sum_{k=0}^{(p-1)/2} 5 \frac{\frac{p-1}{2} - \frac{p-1}{2} - 2k}{c_{\frac{p-1}{2} - 2k}} \right) + i \left( \sum_{k=0}^{(p-1)/2} 5 \frac{\frac{p-1}{2} - \frac{p-1}{2} - 2k}{s_{\frac{p-1}{2} - 2k}} \right)
\]

\[
= 5^{(p-1)/4} \sum_{k=0}^{(p-1)/2} e^{((p-1)/2 - 2k)i\theta}
\]

\[
= 5^{(p-1)/4} e^{((p-1)/2)i\theta} \sum_{k=0}^{(p-1)/2} (e^{-2i\theta})^k
\]

\[
= 5^{(p-1)/4} e^{((p-1)/2)i\theta} \frac{e^{-(p-1)i\theta} - 1}{e^{-2i\theta} - 1}
\]

\[
= 5^{(p-1)/4} \frac{e^{-(p+3)/2)i\theta} - e^{((p-1)/2)i\theta}}{e^{2i\theta} - 1}
\]

\[
= 5^{(p-1)/4} \frac{e^{-(p+3)/2)i\theta} - e^{((p-1)/2)i\theta}}{e^{2i\theta} - 1} \cdot e^{2i\theta} - 1
\]

\[
= 5^{(p-1)/4} \frac{e^{-(p+3)/2)i\theta} + e^{((p-1)/2)i\theta} + e^{-(p-1)/2)i\theta} - e^{((p-1)/2)i\theta}
\]

\[
= 5^{(p-1)/4} \frac{e^{-(p+3)/2)i\theta} + e^{((p-1)/2)i\theta} + e^{-(p-1)/2)i\theta} - e^{((p-1)/2)i\theta}
\]

\[
= 5^{(p-1)/4} \frac{1 - e^{-2i\theta} - e^{2i\theta} + 1}{16}
\]

\[
= 5^{p+3} \frac{2c(p-1)/2}{5(p-1)/4} - \frac{2c(p+3)/2}{5(p+3)/4}
\]

\[
= \frac{16}{5}
\]

\[
= \frac{5c(p-1)/2 - c(p+3)/2}{8}
\]

The recurrence relations defining the \( c_j \)'s and \( s_j \)'s can found by the trigonometric identities \( \cos(0 \cdot \theta) = 1, \sin(0 \cdot \theta) = 0 \), and for \( j \geq 0 \)

\[
\cos((j + 1)\theta) = \cos(j\theta + \theta) = \cos(j\theta) \cos \theta - \sin(j\theta) \sin \theta
\]

\[
\sin((j + 1)\theta) = \sin(j\theta + \theta) = \sin(j\theta) \cos \theta + \cos(j\theta) \sin \theta.
\]

Therefore, \( c_0 = 1, s_0 = 0 \), and for \( j \geq 0 \)

\[
c_{j+1} = c_j - 2s_j \quad \text{and} \quad s_{j+1} = 2c_j + s_j.
\]
The first few values of $c_j$ and $s_j$ are displayed in the following table.

<table>
<thead>
<tr>
<th>$j$</th>
<th>$c_j$</th>
<th>$s_j$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>-3</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>-11</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>-7</td>
<td>-24</td>
</tr>
<tr>
<td>5</td>
<td>41</td>
<td>-38</td>
</tr>
<tr>
<td>6</td>
<td>117</td>
<td>44</td>
</tr>
<tr>
<td>7</td>
<td>29</td>
<td>278</td>
</tr>
<tr>
<td>8</td>
<td>-527</td>
<td>336</td>
</tr>
<tr>
<td>9</td>
<td>-1199</td>
<td>-718</td>
</tr>
<tr>
<td>10</td>
<td>237</td>
<td>-3116</td>
</tr>
<tr>
<td>11</td>
<td>6469</td>
<td>-2642</td>
</tr>
<tr>
<td>12</td>
<td>11753</td>
<td>10296</td>
</tr>
</tbody>
</table>

By solving the recurrence relation for $c_j$ and $s_j$, we have that

$$c_n = \frac{1}{2}(1 + 2i)^n + \frac{1}{2}(1 - 2i)^n.$$ 

Therefore,

$$\frac{5c_{(p-1)/2} - c_{(p+3)/2}}{8} = \frac{1}{16} \left( 5(1 + 2i)^{(p-1)/2} + 5(1 - 2i)^{(p-1)/2} + (1 - 2i)^{(p+3)/2} + (1 - 2i)^{(p+3)/2} \right)$$

$$= \frac{1}{4} \left( (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) \right).$$

This completes the proof of Lemma 5.

**Proof of Theorem 3.**
If \( p \equiv 1 \pmod{40} \), \( p \equiv 9 \pmod{40} \), \( p \equiv 21 \pmod{40} \), or \( p \equiv 29 \pmod{40} \), then \( p \equiv 1 \pmod{4} \), \((5/p) = 1\) and \((-1/p) = 1\). Therefore, by Theorem 2 \( p|F_{(p-1)/2} \). But since \( F_{2n} = L_n F_n \) and \( L_n \) and \( F_n \) have a gcd of either 1 or 2, we have that \( p|L_{(p-1)/4} \) or \( p|F_{(p-1)/4} \) but not both. Using the well-known result,

\[
L_{2n} = L_n^2 - 2(-1)^n
\]

it follows that

\[
L_{\frac{p-1}{4}} = L_{\frac{2}{p-1}}^2 - 2(-1)^{-\frac{p-1}{8}}.
\]

Now if \( p \equiv 1 \pmod{40} \) or \( p \equiv 9 \pmod{40} \) we have that

\[
L_{\frac{p-1}{4}} = L_{\frac{2}{p-1}}^2 - 2.
\]

Using the above identity and then Lemmas 4 and 5 we have that

\[
2^{p-2}\left(L_{\frac{p-1}{4}}^2 - 2\right) = 2^{p-2}L_{\frac{p-1}{2}}
\]

\[
\equiv \frac{(p-1)/2}{5} \sum_{k=0}^{\frac{p-1}{2}-1} \binom{p-1}{2k+1} \binom{p-1}{2} - 2k
\]

\[
\equiv \frac{1}{4} \left(1 + 2i\right)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) \pmod{p}.
\]

Multiplying both sides of the congruence by 4 we have

\[
2^p\left(L_{\frac{p-1}{4}}^2 - 2\right) \equiv (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) \pmod{p}.
\]

Using Fermat’s Little Theorem and simplifying we have

\[
2L_{\frac{p-1}{4}}^2 - 4 \equiv (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) \pmod{p},
\]

\[
2L_{\frac{p-1}{4}}^2 \equiv (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) + 4 \pmod{p},
\]

and

\[
L_{\frac{p-1}{4}} \equiv (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) + 4 \pmod{p}.
\]

This completes the proof of part (a). The proof of part (b) follows by continuing with the well-known identity that

\[
L_{2n} = L_n^2 - 2(-1)^n.
\]
Thus,
\[ L_{\frac{p-1}{4}} = L_{\frac{p+1}{4}}^2 - 2(-1)^{\frac{p-1}{4}}. \]

Now if \( p \equiv 21 \pmod{40} \) or \( p \equiv 29 \pmod{40} \) we have that
\[ L_{\frac{p-1}{4}} = L_{\frac{p+1}{4}}^2 + 2. \]

Using the above identity and then Lemmas 4 and 5 we have that
\[ 2^{p-2}(L_{\frac{p+1}{4}}^2 + 2) = 2^{p-2}L_{\frac{p-1}{4}} \]
\[ = \sum_{k=0}^{(p-1)/2} \frac{2^{\frac{p+1}{4} - \frac{p-1}{4} - 2k}}{5} \]
\[ \equiv \frac{1}{4} \left( (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) \right) \pmod{p}. \]

Multiplying both sides of the congruence by 4 we have
\[ 2^p(L_{\frac{p-1}{4}}^2 + 2) \equiv (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) \pmod{p}. \]

Using Fermat’s Little Theorem and simplifying we have
\[ 2L_{\frac{p-1}{4}}^2 + 4 \equiv (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) \pmod{p}, \]
\[ 2L_{\frac{p+1}{4}}^2 \equiv (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) - 4 \pmod{p}, \]
and \[ L_{\frac{p-1}{4}} \equiv (1 + 2i)^{(p-1)/2}(2 - i) + (1 - 2i)^{(p-1)/2}(2 + i) - 4 \pmod{p}. \]

The theorem follows.

### 3. Examples and Questions

Theorem 3 is useful in determining primes in the Lucas and Fibonacci sequence. For example, by Theorem 3 we have that 29|\( L_7 \), 41|\( L_{10} \), 61|\( F_{15} \), 89|\( F_{22} \), 101|\( L_{25} \), 109|\( F_{27} \), 149|\( F_{37} \), 181|\( L_{45} \), 229|\( L_{57} \), 241|\( L_{60} \), 269|\( F_{67} \), and 281|\( L_{70} \).

There are several questions that remain unanswered.
1. Let \( n \) be a nonnegative integer. Can the expression
\[(1 + 2i)^n(2 - i) + (1 - 2i)^n(2 + i)\]
be simplified?

2. Let \( p \) be a prime such that \( p \equiv 1, 9, 21, \) or \( 29 \pmod{40} \). Prove or disprove that
\[(1 + 2i)^{\frac{p-1}{2}}(2 - i) + (1 - 2i)^{\frac{p-1}{2}}(2 + i) \equiv \pm 4 \pmod{p}.
\]

3. Can Theorem 3 be extended? That is, can we state a theorem for Lucas sequences \( U \) and \( V \).

4. Can we find a theorem similar to Theorem 3 for \( (p \pm 1)/8 \)?

5. What can be said about divisibility properties for third order linear recurrence relations.

We leave all these as open questions.

References


AMS Classification Numbers: 11B39.