Fibonacci Numbers and Modular Arithmetic

The Fibonacci Sequence start with $F_1 = 1$ and $F_2 = 1$. Then the two consecutive numbers are added to find the next term. The Lucas Sequence starts with $L_1 = 1$ and $L_2 = 2$ following the same rule of adding two previous consecutive numbers to find the next term.

Fibonacci Sequence: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144 ...
Lucas Sequence: 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

Recursive Formula: $F_n = F_{n-1} + F_{n-2}$
Recursive Formula: $L_n = L_{n-1} + L_{n-2}$

Table 1

Using Table 1 or the list given, here is an example of how the pattern works. Given $F_1 = 1$, $F_2 = 1$

- $F_3 = F_1 + F_2 = 1 + 1 = 2$
- $F_4 = F_2 + F_3 = 1 + 2 = 3$
- $F_5 = F_3 + F_4 = 2 + 3 = 5$
- $F_6 = F_4 + F_5 = 3 + 5 = 8$

Table 2

<table>
<thead>
<tr>
<th>n</th>
<th>$F_n$</th>
<th>$L_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>13</td>
<td>21</td>
</tr>
<tr>
<td>8</td>
<td>21</td>
<td>34</td>
</tr>
<tr>
<td>9</td>
<td>34</td>
<td>55</td>
</tr>
<tr>
<td>10</td>
<td>55</td>
<td>89</td>
</tr>
<tr>
<td>11</td>
<td>89</td>
<td>144</td>
</tr>
<tr>
<td>12</td>
<td>144</td>
<td>233</td>
</tr>
<tr>
<td>13</td>
<td>233</td>
<td>377</td>
</tr>
</tbody>
</table>

Table 2 (on the right) is a table of fractions each found by the following fraction: $\frac{F_n}{F_{n-1}}$ which are the relative sizes of the Fibonacci numbers. The relative sizes can each be rewritten number called $\varphi$ ("phi") whose precise value is then continued the unending golden ratio as the following examples: $\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \ldots}}}$

Golden Ratio: $\varphi = \frac{1 + \sqrt{5}}{2}$

Example: Rabbits Suppose you begin with a pair of baby rabbits, one male and one female. The rabbits have a 1 month gestation period (1 month being in the womb) and they can reproduce after 1 month of being born. Each pair reproduces another pair. Assume no pair ever dies. How many pairs of rabbits will exist in a particular month?

Pattern:

<table>
<thead>
<tr>
<th>Time in Months</th>
<th>Start</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Pairs</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>8</td>
<td>13</td>
<td>21</td>
</tr>
</tbody>
</table>

Each new month, the number of pairs of new baby equal the number of pair of parents of the previous month. Adults become parents and new babies become adults.*

*New babies refers to those just born. Adults are 1 month olds and ready to reproduce. Parent pairs are those who just gave birth.

Example: New Patterns Determine a simple formula for $(F_n)^2 + (F_{n+1})^2$

<table>
<thead>
<tr>
<th>n</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(F_n)^2$</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>25</td>
<td>64</td>
<td>169</td>
<td>441</td>
</tr>
<tr>
<td>$(F_{n+1})^2$</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>25</td>
<td>64</td>
<td>169</td>
<td>441</td>
<td>1156</td>
</tr>
<tr>
<td>sum</td>
<td>2</td>
<td>5</td>
<td>13</td>
<td>34</td>
<td>89</td>
<td>233</td>
<td>610</td>
<td>1597</td>
</tr>
</tbody>
</table>

Creating tables is a helpful method of identifying patterns that otherwise cannot immediately be seen.
**Fibonacci Numbers and Modular Arithmetic**

**Modular Arithmetic** (informally known as clock arithmetic): In modular arithmetic, numbers “wrap around” upon reaching a given fixed quantity, which is known as the modulus (which would be 12 in the case of hours on a clock). When working with 12 as the modulus, we can say we are working with mod 12.

**Equivalence:** \( \equiv \) means *equivalent* which is not the same as equal.

For example, on a modulus 12 clock, 12 is equivalent to 0; therefore, \( 12 \equiv 0 \mod 12 \) which can be read as “12 is equivalent to 0 mod 12.” Another example is 37 is equivalent to 1. Start at 0 and count up to 37. You should return to 1. Therefore, \( 37 \equiv 1 \mod 12 \).

**Another Perspective** Now suppose we are working with modulus 10. 10, 20, 30, 40, 50, 60, etc are multiples of 10; therefore, they are all equivalent to 0 mod 10. 34 is a multiple of 10 with a remainder of 4; therefore, \( 34 \equiv 4 \mod 10 \).

\[ a \equiv r \mod m \text{ } a \text{ is an integer with a multiple of } m \text{ with a remainder } r. \]

**Check Digits**

The following formulas are used to verify identification numbers using modulus 10.

**Bar Codes**

\[ 3d_1 + d_2 + 3d_3 + d_4 + 3d_5 + d_6 + 3d_7 + d_8 + 3d_9 + d_{10} + 3d_{11} + c \equiv 0 \mod 10 \]

There are 12 digits and \( c \) is the check digit.

**ISBN-13**

\[ d_1 + 3d_2 + d_3 + 3d_4 + d_5 + 3d_6 + d_7 + 3d_8 + d_9 + 3d_{10} + d_{11} + 3d_{12} + d_{13} \equiv 0 \mod 10 \]

The last digit, \( d_{13} \), is the check digit.

**Checks**

\[ 7n_1 + 3n_2 + 9n_3 + 7n_4 + 3n_5 + 9n_6 + 7n_7 + 3n_8 + 9n_9 \equiv 0 \mod 10 \]

The last digit, \( n_9 \) is the check digit.

**Example:** Given the bar code 3 4 0 0 3 2 6 9 1 2 0 6. Find the check digit \( c \).

**Step 1:** Use the formula for bar codes: \( 3(3)+4+3(0)+0+3(3)+2+3(6)+9+3(1)+2+3(0) = 56 \)

**Step 2:** We need \( 56 + c \equiv 0 \mod 10 \) which means we need a multiple of 10 and r=0. Note that \( 56 + 4 = 60 \)

**Step 3:** \( 60 \equiv 0 \mod 10 \). This tells us \( c = 4 \).

**Fermat’s Little Theorem** If \( p \) is a prime number and \( n \) is any integer that does not have \( p \) as a factor then \( n^{p-1} \) is equivalent to 1 mod \( p \). In other words, \( n^{p-1} \) will always have a remainder of 1 when divided by \( p \).

**Notation:** \( n^{p-1} \equiv 1 \mod p \)

**Some Rules**

- If \( a = qm + r \) then \( a \equiv r \mod m \)
- If \( a \equiv r \mod m \) then \( a^k \equiv r^k \mod m \)
- \( a \equiv r \mod m \iff a+b \equiv r+b \mod m \)
- \( a \equiv r \mod m \iff ab \equiv rb \mod m \)

**Simplifying Modulos**

**Example:** Given: \( 5^6 \equiv r \mod 7 \) Find \( r \).

**Step 1:** Use Fermat’s Little Theorem.

We know we are working with \( p = 7 \) and \( p \equiv 1 \mod 7 \) \( 1 = 6 \)

**Step 2:** Confirm 5 does not have a factor of 7.

Therefore, \( 5^7 \equiv 5^6 \equiv 1 \mod 7 \)

**Example:** Given \( 5^{600} \equiv r \mod 7 \). Find \( r \).

**Step 1:** Recall known facts: \( 5^6 \equiv 1 \mod 7 \)

**Step 2:** Manipulate the numbers using known facts and rules:

\[ 5^{600} \equiv (5^6)^{100} \equiv 1^{100} \equiv 1 \mod 7 \]