Divisibility in the Fibonacci Numbers

Stefan Erickson

Colorado College

January 27, 2006

Fibonacci Numbers

$$F_{n+2} = F_{n+1} + F_n$$

n	1	2	3	4	5	6	7	8	9	10	11	12
F_n	1	1	2	3	5	8	13	21	34	55	89	144

n	13	14	15	16	17	18	19	20
F_n	233	377	610	987	1597	2584	4181	6765

n	21	22	23	24	25	26
F_n	10946	17711	28657	46368	75025	121393

n	27	28	29	30	31	32
F_n	196418	317811	514229	832040	1346269	2178309

Lucas Numbers

$$L_{n+2} = L_{n+1} + L_n$$

n	1	2	3	4	5	6	7	8	9	10	11	12
L_n	1	3	4	7	11	18	29	47	76	123	199	322

n	13	14	15	16	17	18	19	20
L_n	521	843	1364	2207	3571	5778	9349	15127

n	21	22	23	24	25	26
L_n	24476	39603	64079	103682	167761	271443

n	27	28	29	30	31	32
L_n	439204	710647	1149851	1860498	3010349	4870847

Fundamental Questions

- Is there a formula for the n^{th} Fibonacci number?
- Which Fibonacci numbers divide other Fibonacci numbers?
- Which primes divide the Fibonacci numbers?
- What is the "entry point" for each prime?
- What about the Lucas numbers?

Recurrence Relations

Guess: $\mathcal{F}_n = r^n$ for some r.

$$\mathcal{F}_{n+2} = \mathcal{F}_{n+1} + \mathcal{F}_n$$

Recurrence Relations

Guess: $\mathcal{F}_n = r^n$ for some r.

$$\mathcal{F}_{n+2} = \mathcal{F}_{n+1} + \mathcal{F}_n$$

$$r^{n+2} = r^{n+1} + r^n$$

$$r^n \cdot (r^2 - r - 1) = 0$$

Recurrence Relations

Guess: $\mathcal{F}_n = r^n$ for some r.

$$\begin{aligned} \mathcal{F}_{n+2} &= \mathcal{F}_{n+1} + \mathcal{F}_n \\ r^{n+2} &= r^{n+1} + r^n \\ r^n \cdot (r^2 - r - 1) &= 0 \\ r_1 = \phi = \frac{1+\sqrt{5}}{2} &= 1.61803398874989484820\ldots \\ r_2 = \phi' = \frac{1-\sqrt{5}}{2} &= -0.61803398874989484820\ldots \end{aligned}$$

Recurrence Relations

Guess: $\mathcal{F}_n = r^n$ for some r.

$$\begin{aligned}
\mathcal{F}_{n+2} &= \mathcal{F}_{n+1} + \mathcal{F}_n \\
r^{n+2} &= r^{n+1} + r^n \\
r^n \cdot (r^2 - r - 1) &= 0 \\
r_1 = \phi = \frac{1+\sqrt{5}}{2} &= 1.61803398874989484820\ldots \\
r_2 = \phi' = \frac{1-\sqrt{5}}{2} &= -0.61803398874989484820\ldots
\end{aligned}$$

$$\phi \cdot \phi' = -1 \qquad \phi^n = F_n \cdot \phi + F_{n-1}$$

Binet's Formula

General Solution:

$$\mathcal{F}_n = c_1 r_1^n + c_2 r_2^n$$

Binet's Formula

General Solution:

$$\mathcal{F}_n = c_1 r_1^n + c_2 r_2^n$$

$$F_0 = 0,\ F_1 = 1 \quad \Longrightarrow \quad c_1 = \frac{1}{\sqrt{5}},\ c_2 = -\frac{1}{\sqrt{5}}$$

$$\boxed{F_n = \frac{1}{\sqrt{5}}\left(\phi^n - \phi'^n\right)}$$

Binet's Formula

General Solution:

$$\mathcal{F}_n = c_1 r_1^n + c_2 r_2^n$$

$$F_0 = 0,\ F_1 = 1 \quad \Longrightarrow \quad c_1 = \tfrac{1}{\sqrt{5}},\ c_2 = -\tfrac{1}{\sqrt{5}}$$

$$\boxed{F_n = \tfrac{1}{\sqrt{5}}\left(\phi^n - \phi'^n\right)}$$

$$L_0 = 2,\ L_1 = 1 \quad \Longrightarrow \quad c_1 = 1,\ c_2 = 1$$

$$\boxed{L_n = \phi^n + \phi'^n}$$

Generating Functions

$$\sum_{n=0}^{\infty} F_n x^n = \frac{x}{1 - x - x^2}$$

Generating Functions

$$\sum_{n=0}^{\infty} F_n x^n = \frac{x}{1 - x - x^2}$$

$$= \frac{x}{(1 - \phi\, x)(1 - \phi' x)}$$

Generating Functions

$$\begin{aligned}
\sum_{n=0}^{\infty} F_n x^n &= \frac{x}{1-x-x^2} \\
&= \frac{x}{(1-\phi\, x)(1-\phi' x)} \\
&= \frac{1}{\sqrt{5}}\;\frac{1}{1-\phi\, x} - \frac{1}{\sqrt{5}}\;\frac{1}{1-\phi' x}
\end{aligned}$$

Generating Functions

$$\begin{aligned}
\sum_{n=0}^{\infty} F_n x^n &= \frac{x}{1-x-x^2} \\
&= \frac{x}{(1-\phi\, x)(1-\phi' x)} \\
&= \frac{1}{\sqrt{5}}\ \frac{1}{1-\phi\, x} - \frac{1}{\sqrt{5}}\ \frac{1}{1-\phi' x} \\
&= \frac{1}{\sqrt{5}}\ \sum_{n=0}^{\infty} (\phi\, x)^n - \frac{1}{\sqrt{5}}\ \sum_{n=0}^{\infty} (\phi' x)^n
\end{aligned}$$

Generating Functions

$$
\begin{aligned}
\sum_{n=0}^{\infty} F_n x^n &= \frac{x}{1-x-x^2} \\
&= \frac{x}{(1-\phi\, x)(1-\phi' x)} \\
&= \frac{1}{\sqrt{5}}\ \frac{1}{1-\phi\, x} - \frac{1}{\sqrt{5}}\ \frac{1}{1-\phi' x} \\
&= \frac{1}{\sqrt{5}}\ \sum_{n=0}^{\infty} (\phi\, x)^n - \frac{1}{\sqrt{5}}\ \sum_{n=0}^{\infty} (\phi' x)^n \\
&= \sum_{n=0}^{\infty} \frac{1}{\sqrt{5}} \left(\phi^n - \phi'^n\right) x^n
\end{aligned}
$$

Consequences

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \lim_{n\to\infty} \frac{L_{n+1}}{L_n} = \phi$$

Consequences

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \lim_{n\to\infty} \frac{L_{n+1}}{L_n} = \phi$$

$$\lim_{n\to\infty} \frac{L_n}{F_n} = \sqrt{5}$$

Consequences

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \lim_{n\to\infty} \frac{L_{n+1}}{L_n} = \phi$$

$$\lim_{n\to\infty} \frac{L_n}{F_n} = \sqrt{5}$$

$$F_{2n} = F_n \cdot L_n$$

Consequences

$$\lim_{n\to\infty}\frac{F_{n+1}}{F_n}=\lim_{n\to\infty}\frac{L_{n+1}}{L_n}=\phi$$

$$\lim_{n\to\infty}\frac{L_n}{F_n}=\sqrt{5}$$

$$F_{2n}=F_n\cdot L_n$$

$$\left(\textbf{Proof.}\quad \frac{1}{\sqrt{5}}\big(\phi^{2n}-\phi'^{2n}\big)=\frac{1}{\sqrt{5}}\big(\phi^{n}-\phi'^{n}\big)\cdot\big(\phi^{n}+\phi'^{n}\big)\right)$$

Super Cool Formula

$$\mathcal{F}_n = \mathcal{F}_{n-1} + \mathcal{F}_{n-2}$$

Super Cool Formula

$$
\begin{aligned}
\mathcal{F}_n &= \mathcal{F}_{n-1} + \mathcal{F}_{n-2} \\
&= (\mathcal{F}_{n-2} + \mathcal{F}_{n-3}) + \mathcal{F}_{n-2} \qquad = 2\,\mathcal{F}_{n-2} + 1\,\mathcal{F}_{n-3}
\end{aligned}
$$

Super Cool Formula

$$\begin{aligned} \mathcal{F}_n &= \mathcal{F}_{n-1} + \mathcal{F}_{n-2} \\ &= (\mathcal{F}_{n-2} + \mathcal{F}_{n-3}) + \mathcal{F}_{n-2} &&= 2\,\mathcal{F}_{n-2} + 1\,\mathcal{F}_{n-3} \\ &= 2\,(\mathcal{F}_{n-3} + \mathcal{F}_{n-4}) + \mathcal{F}_{n-3} &&= 3\,\mathcal{F}_{n-3} + 2\,\mathcal{F}_{n-4} \end{aligned}$$

Super Cool Formula

$$\begin{aligned}
\mathcal{F}_n &= \mathcal{F}_{n-1} + \mathcal{F}_{n-2} \\
&= (\mathcal{F}_{n-2} + \mathcal{F}_{n-3}) + \mathcal{F}_{n-2} &&= 2\,\mathcal{F}_{n-2} + 1\,\mathcal{F}_{n-3} \\
&= 2\,(\mathcal{F}_{n-3} + \mathcal{F}_{n-4}) + \mathcal{F}_{n-3} &&= 3\,\mathcal{F}_{n-3} + 2\,\mathcal{F}_{n-4} \\
&= 3\,(\mathcal{F}_{n-4} + \mathcal{F}_{n-5}) + 2\,\mathcal{F}_{n-4} &&= 5\,\mathcal{F}_{n-4} + 3\,\mathcal{F}_{n-5}
\end{aligned}$$

Super Cool Formula

$$\begin{aligned}
\mathcal{F}_n &= \mathcal{F}_{n-1} + \mathcal{F}_{n-2} \\
&= (\mathcal{F}_{n-2} + \mathcal{F}_{n-3}) + \mathcal{F}_{n-2} && = 2\,\mathcal{F}_{n-2} + 1\,\mathcal{F}_{n-3} \\
&= 2\,(\mathcal{F}_{n-3} + \mathcal{F}_{n-4}) + \mathcal{F}_{n-3} && = 3\,\mathcal{F}_{n-3} + 2\,\mathcal{F}_{n-4} \\
&= 3\,(\mathcal{F}_{n-4} + \mathcal{F}_{n-5}) + 2\,\mathcal{F}_{n-4} && = 5\,\mathcal{F}_{n-4} + 3\,\mathcal{F}_{n-5}
\end{aligned}$$

$$\boxed{F_{m+n} = F_m \cdot F_{n+1} + F_{m-1} \cdot F_n}$$

$$\boxed{L_{m+n} = F_m \cdot L_{n+1} + F_{m-1} \cdot L_n}$$

Theorem. *F_n divides F_{kn} for all integers k.*

Theorem. *F_n divides F_{kn} for all integers k.*

Proof. F_n divides F_n, so the theorem is true for $k = 1$.

Suppose F_n divides F_{kn}. Then

$$F_{(k+1)n} = F_{kn} \cdot F_{n+1} + F_{kn-1} \cdot F_n$$

is also divisible by F_n. By induction, the theorem is true for all k!

Theorem. *F_n divides F_{kn} for all integers k.*

Proof. F_n divides F_n, so the theorem is true for $k = 1$.

Suppose F_n divides F_{kn}. Then

$$F_{(k+1)n} = F_{kn} \cdot F_{n+1} + F_{kn-1} \cdot F_n$$

is also divisible by F_n. By induction, the theorem is true for all k!

Theorem. *L_n divides L_{kn} for all <u>odd</u> integers k.*

Theorem. *F_n divides F_{kn} for all integers k.*

Proof. F_n divides F_n, so the theorem is true for $k = 1$.

Suppose F_n divides F_{kn}. Then

$$F_{(k+1)n} = F_{kn} \cdot F_{n+1} + F_{kn-1} \cdot F_n$$

is also divisible by F_n. By induction, the theorem is true for all k!

Theorem. *L_n divides L_{kn} for all <u>odd</u> integers k.*

Proof. Same proof, except

$$L_{(2l+1)n} = F_{2ln} \cdot L_{n+1} + F_{2ln-1} \cdot L_n$$

and L_n divides F_{2n}, which in turn divides F_{2ln}.

Greatest Common Divisors

Theorem. $\gcd(F_m, F_n) = F_{\gcd(m,n)}$. Ex: $\gcd(144, 2584) = 8$.

Greatest Common Divisors

Theorem. $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.   Ex: $\gcd(144, 2584) = 8$.

Proof. Let $d = \gcd(m, n)$. By the previous theorem, F_d divides F_m and F_n. Thus, F_d divides $\gcd(F_m, F_n)$.

Greatest Common Divisors

Theorem. $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.   Ex: $\gcd(144, 2584) = 8$.

Proof. Let $d = \gcd(m, n)$. By the previous theorem, F_d divides F_m and F_n. Thus, F_d divides $\gcd(F_m, F_n)$.

d may be written as $am + bn$ for some integers a and b. Then

$$F_d = F_{am+bn} = F_{am} \cdot F_{bn+1} + F_{am-1}F_{bn}$$

Since F_m divides F_{am} and F_n divides F_{bn}, F_d can be written as a linear combination of F_m and F_n. Hence, $\gcd(F_m, F_n)$ divides F_d.

Question: Which Fibonacci numbers divide other Fibonacci numbers?

Answer: F_n divides F_m if and only if n divides m.

Question: Which Fibonacci numbers divide other Fibonacci numbers?

Answer: F_n divides F_m if and only if n divides m.

For example, the Fibonacci numbers which divide $F_{30} = 832040$ are $F_3 = 2$, $F_5 = 5$, $F_6 = 8$, $F_{10} = 55$, and $F_{15} = 610$.

Question: Which Fibonacci numbers divide other Fibonacci numbers?

Answer: F_n divides F_m if and only if n divides m.

For example, the Fibonacci numbers which divide $F_{30} = 832040$ are $F_3 = 2$, $F_5 = 5$, $F_6 = 8$, $F_{10} = 55$, and $F_{15} = 610$.

In order for F_n to be prime, n must be prime. The converse is *not* true, since $F_{19} = 4181 = 37 \cdot 113$.

Prime Divisibility

Question: Which primes divide the Fibonacci numbers?

Prime Divisibility

Question: Which primes divide the Fibonacci numbers?

Answer: All of them! If $p \neq 5$, then p divides either F_{p-1} or F_{p+1}.

Prime Divisibility

Question: Which primes divide the Fibonacci numbers?

Answer: All of them! If $p \neq 5$, then p divides either F_{p-1} or F_{p+1}.

For example, 7 divides $F_8 = 21$ and 11 divides $F_{10} = 55$.

Note that $F_5 = 5$ is the only exception.

Lemma.

$$\phi^p \equiv \begin{cases} \phi \pmod{p} & \textit{if } p \equiv 1, 4 \pmod{5} \\ \phi' \pmod{p} & \textit{if } p \equiv 2, 3 \pmod{5} \end{cases}$$

Lemma.

$$\phi^p \equiv \begin{cases} \phi \pmod{p} & \textit{if } p \equiv 1, 4 \pmod{5} \\ \phi' \pmod{p} & \textit{if } p \equiv 2, 3 \pmod{5} \end{cases}$$

Proof.

$$\phi^p = \frac{1}{2^p}\left(1 + \sqrt{5}\right)^p$$

Lemma.

$$\phi^p \equiv \begin{cases} \phi \pmod p & \textit{if } p \equiv 1, 4 \pmod 5 \\ \phi' \pmod p & \textit{if } p \equiv 2, 3 \pmod 5 \end{cases}$$

Proof.

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

Lemma.

$$\phi^p \equiv \begin{cases} \phi \pmod{p} & \textit{if } p \equiv 1, 4 \pmod{5} \\ \phi' \pmod{p} & \textit{if } p \equiv 2, 3 \pmod{5} \end{cases}$$

Proof.

$$\begin{aligned} \phi^p &= \frac{1}{2^p}\big(1+\sqrt{5}\big)^p \\ &= \frac{1}{2^p}\left(1 + \tbinom{p}{1}\sqrt{5} + \cdots + \tbinom{p}{p-1}\big(\sqrt{5}\big)^{p-1} + \big(\sqrt{5}\big)^p\right) \\ &\equiv \frac{1}{2}\Big(1 + 5^{\frac{p-1}{2}}\sqrt{5}\Big) \pmod{p} \end{aligned}$$

Lemma.

$$\phi^p \equiv \begin{cases} \phi \pmod{p} & \textit{if } p \equiv 1, 4 \pmod{5} \\ \phi' \pmod{p} & \textit{if } p \equiv 2, 3 \pmod{5} \end{cases}$$

Proof.

$$\begin{aligned} \phi^p &= \frac{1}{2^p}\big(1+\sqrt{5}\big)^p \\ &= \frac{1}{2^p}\left(1 + \tbinom{p}{1}\sqrt{5} + \cdots + \tbinom{p}{p-1}\big(\sqrt{5}\big)^{p-1} + \big(\sqrt{5}\big)^p\right) \\ &\equiv \frac{1}{2}\left(1 + 5^{\frac{p-1}{2}}\sqrt{5}\right) \equiv \frac{1}{2}\left(1 + \left(\frac{5}{p}\right)\sqrt{5}\right) \pmod{p} \end{aligned}$$

Lemma.

$$\phi^p \equiv \begin{cases} \phi \pmod{p} & \textit{if } p \equiv 1, 4 \pmod{5} \\ \phi' \pmod{p} & \textit{if } p \equiv 2, 3 \pmod{5} \end{cases}$$

Proof.

$$\begin{aligned} \phi^p &= \frac{1}{2^p}\left(1+\sqrt{5}\right)^p \\ &= \frac{1}{2^p}\left(1+\binom{p}{1}\sqrt{5}+\cdots+\binom{p}{p-1}\left(\sqrt{5}\right)^{p-1}+\left(\sqrt{5}\right)^p\right) \\ &\equiv \frac{1}{2}\left(1+5^{\frac{p-1}{2}}\sqrt{5}\right) \equiv \frac{1}{2}\left(1+\left(\frac{5}{p}\right)\sqrt{5}\right) \pmod{p} \end{aligned}$$

$\left(\frac{5}{p}\right) = 1$ if $p \equiv 1, 4 \pmod{5}$ and $\left(\frac{5}{p}\right) = -1$ if $p \equiv 2, 3 \pmod{5}$.

Theorem.

- *p divides F_{p-1} if* $p \equiv 1, 4 \pmod 5$. (Ex: $11 \mid F_{10} = 55$.)
- *p divides F_{p+1} if* $p \equiv 2, 3 \pmod 5$. (Ex: $7 \mid F_8 = 21$.)

Theorem.

- *p divides F_{p-1} if $p \equiv 1, 4 \pmod 5$.*   (Ex: $11 \mid F_{10} = 55$.)
- *p divides F_{p+1} if $p \equiv 2, 3 \pmod 5$.*   (Ex: $7 \mid F_8 = 21$.)

Proof. If $p \equiv 1, 4 \pmod 5$, then $\phi^p \equiv \phi \pmod p$. Dividing by ϕ, $\phi^{p-1} \equiv 1 \pmod p$.

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

Theorem.

- *p divides F_{p-1} if $p \equiv 1, 4 \pmod 5$.* (Ex: $11 \mid F_{10} = 55$.)
- *p divides F_{p+1} if $p \equiv 2, 3 \pmod 5$.* (Ex: $7 \mid F_8 = 21$.)

Proof. If $p \equiv 1, 4 \pmod 5$, then $\phi^p \equiv \phi \pmod p$. Dividing by ϕ, $\phi^{p-1} \equiv 1 \pmod p$.

$$F_{p-1} = \tfrac{1}{\sqrt{5}}\big(\phi^{p-1} - \phi'^{p-1}\big) \equiv \tfrac{1}{\sqrt{5}}\big(1 - 1\big) \equiv 0 \pmod p.$$

If $p \equiv 2, 3 \pmod 5$, then $\phi^p \equiv \phi' \pmod p$. Multiplying by ϕ, $\phi^{p+1} \equiv -1 \pmod p$.

$$F_{p+1} = \tfrac{1}{\sqrt{5}}\big(\phi^{p+1} - \phi'^{p+1}\big) \equiv \tfrac{1}{\sqrt{5}}\big(-1 + 1\big) \equiv 0 \pmod p.$$

Theorem. *If* p^k *divides* F_n *for some* $k \geq 1$*, then* p^{k+1} *divides* F_{pn}*.*

Theorem. *If p^k divides F_n for some $k \geq 1$, then p^{k+1} divides F_{pn}.*

Proof. Homework problem.

Theorem. *If p^k divides F_n for some $k \geq 1$, then p^{k+1} divides F_{pn}.*

Proof. Homework problem.

Corollary. *Every positive integer divides F_n for some n.*

For example, $1000 = 8 \cdot 125$ divides $F_{6 \cdot 125} = F_{750}$.

Entry Points

The smallest n such that p divides $\mathcal{F}_n$ is called the *entry point* of p.

We use $e_F(p)$ for the entry point of p into the Fibonacci numbers and $e_L(p)$ for the entry point of p into the Lucas numbers.

Entry Points

The smallest n such that p divides $\mathcal{F}_n$ is called the *entry point* of p.

We use $e_F(p)$ for the entry point of p into the Fibonacci numbers and $e_L(p)$ for the entry point of p into the Lucas numbers.

From the previous theorem, $e_F(p)$ divides either $p-1$ or $p+1$.

For example, we know that 13 divides the 14^{th} Fibonacci number. However, 13 also divides $F_7 = 13$, so $e_F(13) = 7$.

On the other hand, 13 does not divide *any* Lucas number. We say that $e_L(13)$ is undefined in this case.

Entry Points for the Lucas Numbers

- If $e_F(p)$ is even, then $e_L(p) = \frac{e_F(p)}{2}$.
- If $e_F(p)$ is odd, then p does not divide any Lucas number.

This follows from $F_{2n} = F_n \cdot L_n$.

For example, $e_F(29) = 14$ and $e_L(29) = 7$.

Question: Which primes divide the Lucas numbers?

One More Formula

$$\boxed{L_n^2 - 5\,F_n^2 = 4 \cdot (-1)^n}$$

One More Formula

$$\boxed{L_n^2 - 5\,F_n^2 = 4 \cdot (-1)^n}$$

Lemma. *If p does not divide L_n for any n, then $p \equiv 1 \pmod 4$.*

Proof. Suppose $n = e_F(p)$ is odd, that is, $p \mid F_n$ for some odd n.

$L_n^2 \equiv -4 \pmod p \implies -1$ is a square mod $p \implies p \equiv 1 \pmod 4$.

One More Formula

$$\boxed{L_n^2 - 5\,F_n^2 = 4 \cdot (-1)^n}$$

Lemma. *If p does not divide L_n for any n, then $p \equiv 1 \pmod{4}$.*

Proof. Suppose $n = e_F(p)$ is odd, that is, $p \mid F_n$ for some odd n.

$L_n^2 \equiv -4 \pmod{p} \implies -1$ is a square mod $p \implies p \equiv 1 \pmod{4}$.

Corollary. *All primes $p \equiv 3 \pmod{4}$ divide the Lucas numbers.*

$$\boxed{L_n^2 - 5\,F_n^2 = 4 \cdot (-1)^n}$$

Lemma. *If* $p \equiv 1 \pmod 4$ *and* $p \equiv 2, 3 \pmod 5$, *then* p *does not divide* L_n *for any* n.

$$\boxed{L_n^2 - 5\,F_n^2 = 4 \cdot (-1)^n}$$

Lemma. *If $p \equiv 1 \pmod 4$ and $p \equiv 2, 3 \pmod 5$, then p does not divide L_n for any n.*

Proof. Suppose $p \mid L_n$. Then

$$-5\,F_n^2 \equiv 4 \cdot (-1)^n \pmod p \implies \pm 5 \text{ is a square mod } p.$$

By quadratic reciprocity, ± 5 are not squares when $p \equiv 1 \pmod 4$ and $p \equiv 2, 3 \pmod 5$.

	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$p \equiv 1, 4 \pmod 5$		
$p \equiv 2, 3 \pmod 5$		

	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$p \equiv 1, 4 \pmod 5$		$p \mid L_n$ for some n
$p \equiv 2, 3 \pmod 5$		$p \mid L_n$ for some n

	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$p \equiv 1, 4 \pmod 5$		$p \mid L_n$ for some n
$p \equiv 2, 3 \pmod 5$	$p \nmid L_n$ for any n	$p \mid L_n$ for some n

	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$p \equiv 1, 4 \pmod 5$	?	$p \mid L_n$ for some n
$p \equiv 2, 3 \pmod 5$	$p \nmid L_n$ for any n	$p \mid L_n$ for some n

Suppose $p \equiv 1 \pmod 4$ and $p \equiv 1, 4 \pmod 5$ such that $p \mid L_n$ for some n. We may assume $n \mid \frac{p-1}{2}$. Then

$$\begin{aligned} L_n = \phi^n + \phi'^n \equiv 0 & \pmod p \\ \phi^n \equiv -\phi'^n & \pmod p \\ \phi^{2n} \equiv (-1)^{n+1} & \pmod p \end{aligned}$$

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

If $n = \frac{p-1}{4}$ is odd, then $\phi^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ means ϕ is a square mod p. Hence, $\frac{1}{2}$ of the primes $p \equiv 5 \pmod{8}$ divide $L_{\frac{p-1}{4}}$.

If $n = \frac{p-1}{4}$ is even, then $\phi^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ means ϕ is not a square mod p. Hence, $\frac{1}{2}$ of the primes $p \equiv 1 \pmod{8}$ divide $L_{\frac{p-1}{4}}$.

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

If $n = \frac{p-1}{8}$ is odd, then $\phi^{\frac{p-1}{4}} \equiv 1 \pmod{p}$ means ϕ is a fourth power mod p. Hence, $\frac{1}{4}$ of the primes $p \equiv 9 \pmod{16}$ divide $L_{\frac{p-1}{8}}$.

If $n = \frac{p-1}{8}$ is even, then $\phi^{\frac{p-1}{4}} \equiv -1 \pmod{p}$ means ϕ is a square but not a fourth power mod p. Hence, $\frac{1}{4}$ of the primes $p \equiv 1 \pmod{16}$ divide $L_{\frac{p-1}{8}}$.

Question: How many primes divide the Lucas numbers?

Answer:

$$\frac{1}{2} + \frac{1}{8} + \frac{1}{32} + \frac{1}{128} + \cdots = \frac{1}{2} \cdot \sum_{n=0}^{\infty} \left(\frac{1}{4}\right)^n = \frac{2}{3}$$

The density of the primes dividing the Lucas numbers is $\frac{2}{3}$!

Conclusions

- F_n divides F_m if and only if n divides m.
-
-
-
-

Conclusions

- F_n divides F_m if and only if n divides m.
- L_n divides L_m if and only if m is an odd multiple of n.
-
-
-

Conclusions

- F_n divides F_m if and only if n divides m.
- L_n divides L_m if and only if m is an odd multiple of n.
- Every positive integer divides the Fibonacci numbers.
-
-

Conclusions

- F_n divides F_m if and only if n divides m.
- L_n divides L_m if and only if m is an odd multiple of n.
- Every positive integer divides the Fibonacci numbers.
- $\frac{2}{3}$ of the primes divide the Lucas numbers.
-

Conclusions

- F_n divides F_m if and only if n divides m.
- L_n divides L_m if and only if m is an odd multiple of n.
- Every positive integer divides the Fibonacci numbers.
- $\frac{2}{3}$ of the primes divide the Lucas numbers.
- The Fibonacci and Lucas numbers are cool!