

On the Divisibility of the Lucas Sequence

By:

Syrous Marivani

LSUA

Mathematics Department

Alexandria, LA 71302

The so-called Lucas sequence ([3]) $\{g(n)\}_{n \geq 0}$ satisfies the recurrence relation:

$$g(n) = g(n-1) + g(n-2), \quad (1)$$

where $g(0) = 2$, and $g(1) = 1$. The following table describes the behaviors of

$\{g(n)\}_{0 \leq n \leq 20}$, mod p , where p is a prime, $2 \leq p \leq 11$.

Table 1

n	$g(n)$	$g(n) \bmod 2$	$g(n) \bmod 3$	$g(n) \bmod 5$	$g(n) \bmod 7$	$g(n) \bmod 11$
0	2	0	-1	2	2	2
1	1	1	1	1	1	1
2	3	1	0	3	3	3
3	4	0	1	-1	-3	-3
4	7	1	1	2	0	-4
5	11	1	-1	1	-3	0
6	18	0	0	3	4	-4
7	29	1	-1	-1	1	-4
8	47	1	-1	2	-2	3
9	76	0	1	1	-1	-1

10	123	1	0	-2	-3	2
11	199	1	1	-1	3	1
12	322	0	1	2	0	3
13	521	1	2	1	3	4
14	843	1	0	-2	3	-4
15	1364	0	-1	-1	-1	0
16	2207	1	-1	2	2	-4
17	3571	1	1	1	1	-4
18	5778	0	0	-2	3	3
19	9349	1	1	-1	-3	-1
20	15127	1	1	2	0	2

A moment of observation shows that for example:

$$n \equiv 0 \pmod{3}, \text{ then } g(n) \equiv 0 \pmod{2},$$

$$n \equiv 2 \pmod{4}, \text{ then } g(n) \equiv 0 \pmod{3},$$

$$g(n) \text{ is never congruent to } 0 \pmod{5},$$

$$n \equiv 4 \pmod{8}, \text{ then } g(n) \equiv 0 \pmod{7},$$

$$n \equiv 5 \pmod{10}, \text{ then } g(n) \equiv 0 \pmod{11}.$$

These observations can be proven, for example I prove the last assertion. Suppose $g(n) \equiv 0 \pmod{11}$, then by repeated application of the recurrence relation (1) it follows that:

$$g(n + 10) = 55g(n + 1) + 34g(n).$$

From this it follows that:

$$g(n + 10) \equiv 0 \pmod{11} \text{ if and only if } g(n) \equiv 0 \pmod{11}. \quad (2)$$

Since $g(5) \equiv 0 \pmod{11}$, and $g(k)$ is not divisible by 11 for $1 \leq k \leq 4$, then by repeated

application of the latter result it follows that $g(n) \equiv 0 \pmod{11}$, if and only if $n \equiv 5 \pmod{10}$.

The Fibonacci sequence ([2]) $\{f(n)\}_{n \geq 0}$ is a sequence of integers that satisfies the recurrence relation:

$$f(n) = f(n - 1) + f(n - 2)$$

subject to initial conditions $f(0) = 0$, and $f(1) = 1$. These results for primes p , $2 \leq p < 100$, are summarized in Table 2. This table gives the values of p_0 such that if $n \equiv 0 \pmod{p_0}$ then $f(n) \equiv 0 \pmod{p}$ (See [1]).

Table 2

p	and	p_0	p	and	p_0	p	and	p_0
2		3	3		4	5		5
7		8	11		10	13		7
17		9	19		18	23		24
29		14	31		30	37		19
41		20	43		44	47		16
53		27	59		58	61		15
67		68	71		70	73		37
79		78	83		84	89		11
97		49						

This table was obtained by using Maple 7.

Fibonacci and Lucas sequences are special cases of the Generalized Fibonacci sequence.

The Generalized Fibonacci sequence $\{F(n)\}_{n \geq 0}$ is a sequence of integers that satisfies the recurrence relation:

$$F(n) = F(n - 1) + F(n - 2)$$

Theorem 1: If $\{f(n)\}_{n \geq 0}, \{F(n)\}_{n \geq 0}$ are the Fibonacci and Generalized Fibonacci sequences, p is a prime such that p does not divide $F(0)$, and a, p_0 are the least positive integers such that $F(a) \equiv 0 \pmod{p}$ and $f(p_0) \equiv 0 \pmod{p}$, then $F(n) \equiv 0 \pmod{p}$ if and only if $n \equiv a \pmod{p_0}$.

Proof : One can easily show by induction on k that:

$$F(n + k) = f(k)F(n + 1) + f(k - 1)F(n). \quad (3)$$

So if $f(p_0) \equiv 0 \pmod{p}$, and $F(a) \equiv 0 \pmod{p}$, then from (3) it follows that:

$$F(a + k) \equiv 0 \pmod{p} \text{ if and only if } f(k) \equiv 0 \pmod{p} \quad (4)$$

Since $f(n)$ is not congruent to $0 \pmod{p}$ for $1 \leq n < p_0$, then by ([1]), $f(k) \equiv 0 \pmod{p}$ if and only if $k \equiv 0 \pmod{p_0}$. So since $F(n)$ is not congruent to 0 for $1 \leq n < a$, it follows that from (4) that $F(n) \equiv 0 \pmod{p}$ if and only if $n \equiv a \pmod{p_0}$. ♦

From now on p_0 denotes the smallest positive integer such that $f(p_0) \equiv 0 \pmod{p}$. The following are results proven in ([1]).

Theorem 2: If p is an odd prime such that $p \equiv 2, \text{ or } 3 \pmod{5}$, then p_0 divides $p + 1$, if $p \equiv 1, \text{ or } 4 \pmod{5}$ then p_0 divides $p - 1$, and if $p = 5$, then $p_0 = p$.

Corollary 1: $p_0 \mid (p + 1)/2$ if and only if $p \equiv 13, \text{ or } 17 \pmod{20}$.

Corollary 2 : If $p \equiv 2, \text{ or } 3 \pmod{5}$, then p_0 does not divide $(p + 1)/2$ if and only if $p \equiv 3, \text{ or } 7 \pmod{20}$.

Corollary 3 : $p_o \mid (p - 1)/2$ if and only if $p \equiv 1$ or $9 \pmod{20}$.

Corollary 4: Suppose p_o does not divide $(p - 1)/2$ if and only if $p \equiv 11$, or $19 \pmod{20}$.

The following is the analog of Theorem 1 for the Lucas sequence.

Theorem 3: If p is an odd prime and p_o is even, then $g(n) \equiv 0 \pmod{p}$ if and only if

$$n \equiv \frac{p_o}{2} \pmod{p_o}.$$

Proof: Let a be the integer of Theorem 1. If $g(a) \equiv 0 \pmod{p}$, then since ([2], [3]) $f(2a) = f(a)g(a)$, it follows that $f(2a) \equiv 0 \pmod{p}$. By Theorem 1 in ([1]), this is possible if and only if $2a \equiv 0 \pmod{p_o}$. If p_o is odd this is impossible, since the latter implies $a = p_o$. But then using the identity ([2], [3]):

$$5f^2(n) - g^2(n) = -4(-1)^n$$

with $n = p_o$ implies $p = 2$ which is a contradiction. But if p_o is even, this would only imply $a = \frac{p_o}{2}$. So the conclusion of the Theorem follows. ♦

From the proof of this Theorem, it follows that:

Corollary 1: If p_o is odd, there is no integer n such that $g(n) \equiv 0 \pmod{p}$.

I think, with further study, the results here can be extended. Right now, my efforts are in this direction.

References

[1] Syrous Marivani, "On the Fibonacci Sequence" MAA Proceedings, 2003 at

<http://www.mc.edu/campus/users/travis/maa/proceedings/>

[2] Eric W. Weisstein, Fibonacci Number - from Math World at

<http://mathworld.wolfram.com/FibonacciNumber.html>

[3] Eric W. Weisstein, Lucas Number - from Math World at

<http://mathworld.wolfram.com/LucasNumber.html>