

# On the Fibonacci Sequence

By:

Syrous Marivani

LSUA

Mathematics Department

Alexandria, LA 71302

The so-called Fibonacci sequence  $\{f(n)\}_{n \geq 0}$  given by:

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

where  $f(0) = 0$ , and  $f(1) = 1$ . The following table describes the behaviors of  $\{f(n)\}_{0 \leq n \leq 20}$ , mod  $p$ , where  $p$  is a prime,  $2 \leq p \leq 11$ .

**Table 1**

n	f(n)	f(n)mod 2	f(n)mod 3	f(n)mod 5	f(n)mod 7	f(n)mod 11
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	1	1	1	1	1	1
3	2	0	-1	2	2	2
4	3	1	0	-2	3	3
5	5	1	-1	0	-2	5
6	8	0	-1	-2	1	-3
7	13	1	1	-2	-1	2
8	21	1	0	1	0	-1
9	34	0	1	-1	-1	1

10	55	1	1	0	-1	0
11	89	1	-1	-1	-2	1
12	144	0	0	-1	-2	1
13	233	1	-1	-2	2	2
14	377	1	-1	2	-1	3
15	610	0	1	0	1	5
16	987	1	0	2	0	-3
17	1597	1	1	2	1	2
18	2584	0	1	-1	1	-1
19	4181	1	-1	1	2	1
20	6765	1	0	0	3	0

A moment observation shows that if for example:

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

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

$$n \equiv 0 \pmod{5}, \text{ then } f(n) \equiv 0 \pmod{5},$$

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

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

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

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

From this it follows that:

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

Since  $f(0) = 0$ , and  $f(k)$  is not divisible by 11 for  $1 \leq k \leq 9$ , then by repeated application

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

**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. For a prime such as  $p = 6007$ ,  $p_0 = 6008$  and it takes .477 seconds to get this answer.

**Theorem 1:** If  $\{f(n)\}_{n \geq 0}$  is the Fibonacci sequence,  $p$  a prime, and  $p_0$  is the least positive integer such that  $f(p_0) \equiv 0 \pmod{p}$ , then  $f(n) \equiv 0 \pmod{p}$  if and only if  $n \equiv 0 \pmod{p_0}$ .

**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  $f(p_0) \equiv 0 \pmod{p}$ , then:

$$f(n+p_0) \equiv 0 \pmod{p} \text{ if and only if } f(n) \equiv 0 \pmod{p}. \quad (4)$$

Since  $f(n)$  is not congruent to  $0 \pmod p$  for  $1 \leq n < p_0$ , then using (4) the conclusion follows. ♦

From now on  $p_0$  denotes the smallest positive integer such that  $f(p_0) \equiv 0 \pmod p$ .

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

**Proof :** By [1, page 9] we have:

$$f(n) = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right]. \quad (5)$$

Then:

$$2^p f(p+1) = \sum_{i=0}^{(p-1)/2} \binom{p+1}{2i+1} 5^i.$$

Since

$$p \mid \binom{p+1}{2i+1}, \text{ for } 1 \leq i \leq (p-3)/2,$$

then

$$2^p f(p+1) \equiv (1 + 5^{(p-1)/2})(p+1) \pmod p.$$

Using Euler's criterion and the Quadratic reciprocity law [2, Chapter 9, Theorems 9.2 and 9.8] we have:

$$f(p+1) \equiv 0 \pmod p \text{ if and only if } p \equiv 2, \text{ or } 3 \pmod 5. \quad (6)$$

Otherwise using Fermat's theorem [2, Chapter 5, Theorem 5.19] we have:

$$f(p+1) \equiv 1 \pmod p \text{ if and only if } p \equiv 1, \text{ or } 4 \pmod 5. \quad (7)$$

Again using (5) we have:

$$2^{p-1} f(p) \equiv 5^{(p-1)/2} \pmod p, \quad (8)$$

and using [2, Chapter 5, Theorem 5.18] as before :

$$f(p) \equiv 1 \pmod{p} \text{ if and only if } p \equiv 1, \text{ or } 4 \pmod{5}. \quad (9)$$

Since

$$f(p-1) = f(p+1) - f(p),$$

then using (7) and (9), it follows:

$$f(p-1) \equiv 0 \pmod{p} \text{ if only if } p \equiv 1, \text{ or } 4 \pmod{5}. \quad (10)$$

Using (6), (10), and Theorem 1 the assertion of the theorem follows. The case  $p = 5$  follows from (8). ♦

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

**Proof :** Using (8) as before we have:

$$f(p) \equiv -1 \pmod{p} \text{ if } p \equiv 2, \text{ or } 3 \pmod{5}. \quad (11)$$

Using (3) with  $n = \frac{p-1}{2}$ , and  $k = \frac{p+1}{2}$ , we have:

$$f(p) = \left\{ f\left(\frac{p+1}{2}\right) \right\}^2 + \left\{ f\left(\frac{p-1}{2}\right) \right\}^2. \quad (12)$$

Suppose  $p \equiv 2, \text{ or } 3 \pmod{5}$  and  $p_0 \mid (p+1)/2$ , then using (11) and (12) and Theorem 2 we have:

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

This shows that  $-1$  is a quadratic residue mod  $p$ , and so by [2, Chapter 9, Theorem 9.4] we should have  $p \equiv 1 \pmod{4}$ . So  $p_0 \mid (p+1)/2$  if in addition to  $p \equiv 2, \text{ or } 3 \pmod{5}$ , we should have  $p \equiv 1 \pmod{4}$ . Then the conclusion follows from here.

To prove it in the other direction suppose  $p \equiv 13, \text{ or } 17 \pmod{20}$  but  $p_0$  does not divide

$(p + 1)/2$ . Since  $f(p + 1) \equiv 0 \pmod{p}$ , using (3) with  $n = k = \frac{p+1}{2}$ , then:

$$f(p + 1) = f\left(\frac{p+1}{2}\right) \left[ f\left(\frac{p+3}{2}\right) + f\left(\frac{p-1}{2}\right) \right] = f\left(\frac{p+1}{2}\right) \left[ f\left(\frac{p+1}{2}\right) + 2f\left(\frac{p-1}{2}\right) \right].$$

This implies:

$$f\left(\frac{p+1}{2}\right) \equiv -2f\left(\frac{p-1}{2}\right) \pmod{p}. \quad (13)$$

Using (13) in (12) we have:

$$5f^2\left(\frac{p-1}{2}\right) \equiv -1 \pmod{p}.$$

This implies  $-5$  is a quadratic residue mod  $p$ . So  $(-5 | p) = 1$ . This implies  $(5 | p) = 1$ , since  $(-1 | p) = 1$ . This is impossible if  $p \equiv 13, \text{ or } 17 \pmod{20}$ . So  $p_0$  divides  $(p + 1)/2$ . ♦

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

**Proof :** This follows as in the previous Corollary except we should have  $p \equiv -1 \pmod{4}$ , and  $p \equiv 2, \text{ or } 3 \pmod{5}$ . ♦

**Corollary 3 :**  $p_0 | (p - 1)/2$  if and only if  $p \equiv 1 \text{ or } 9 \pmod{20}$ .

**Proof :** Suppose  $p_0 | (p - 1)/2$ . This implies  $p \equiv 1, 4 \pmod{5}$  and we have:

$$f\left(\frac{p-5}{2}\right) \equiv -f\left(\frac{p-3}{2}\right), \quad f\left(\frac{p-7}{2}\right) \equiv 2f\left(\frac{p-3}{2}\right), \quad f\left(\frac{p-9}{2}\right) \equiv -3f\left(\frac{p-3}{2}\right),$$

and in general:

$$f\left(\frac{p-1}{2} - k\right) \equiv (-1)^{k+1} f(k) f\left(\frac{p-3}{2}\right). \quad (14)$$

Letting  $k = (p - 3)/2$  in (14), we have:

$$f^2\left(\frac{p-3}{2}\right) \equiv (-1)^{(p-1)/2} \pmod{p}. \quad (15)$$

Using the results of Theorem 1, it follows that  $f(p-2) \equiv 1 \pmod{p}$ . Using this result and

(3) with  $n = \frac{p-3}{2}$ , and  $k = \frac{p-1}{2}$  we have:

$$f^2\left(\frac{p-3}{2}\right) \equiv 1 \pmod{p}. \quad (16)$$

Using (15) and (16) we conclude  $p \equiv 1 \pmod{4}$ . So since also  $p \equiv 1$  or  $4 \pmod{5}$ , then  $p \equiv 1$  or  $9 \pmod{20}$ .

On the other hand suppose  $p \equiv 1$  or  $9 \pmod{20}$  and  $p_0$  does not divide  $(p-1)/2$ . Since

$f(p-1) \equiv 0 \pmod{p}$  using (3) with  $n = k = \frac{p-1}{2}$ , we have:

$$f(p-1) = f\left(\frac{p-1}{2}\right) \left[ f\left(\frac{p+1}{2}\right) + f\left(\frac{p-3}{2}\right) \right],$$

this implies:

$$f\left(\frac{p+1}{2}\right) \equiv -f\left(\frac{p-3}{2}\right), f\left(\frac{p-1}{2}\right) \equiv -2f\left(\frac{p-3}{2}\right), \text{ and } f\left(\frac{p-5}{2}\right) \equiv -3f\left(\frac{p-3}{2}\right) \pmod{p}, \quad (17)$$

and in general:

$$f\left(\frac{p-3}{2} - k\right) \equiv (-1)^k g(k+1) f\left(\frac{p-3}{2}\right) \pmod{p}, \quad (18)$$

for  $k=0, 1, 2, \dots, (p-3)/2$ , where  $\{g(k)\}_{k \geq 1}$  is the Lucas sequence.

It turns out that:

$$g(n) = \alpha^n + \beta^n; \quad f(n) = (\alpha^n - \beta^n) / \sqrt{5}, \quad (19)$$

where

$$\alpha = (1 + \sqrt{5}) / 2, \text{ and } \beta = (1 - \sqrt{5}) / 2.$$

Letting  $k = (p - 5)/2$  in (18) and using (19) we have:

$$f\left(\frac{p-3}{2}\right)g\left(\frac{p-3}{2}\right) = f(p-3) \equiv (-1)^{(p-5)/2} \pmod{p}. \quad (20)$$

Using the results of Theorem 1 again,  $f(p-3) \equiv -1 \pmod{p}$ . However (20) contradicts this result since  $p \equiv 1, \text{ or } 9 \pmod{20}$ . So  $p_0$  has to divide  $(p-1)/2$ . ♦

**Corollary 4:**  $p_0$  does not divide  $(p-1)/2$  if and only if  $p \equiv 11, \text{ or } 19 \pmod{20}$ .

**Proof :** In this case in addition to  $p \equiv 1, \text{ or } 4 \pmod{5}$  we should have  $p \equiv -1 \pmod{4}$ , from which the conclusion follows. ♦

Using methods similar to these, I think it is possible to know more about  $p_0$ , for instance, when  $p_0 \mid (p+1)/3$ , or  $p_0 \mid (p-1)/3$ , and so on. Right now I have concentrated my efforts in these directions.

## References

- [1] N. N. Vorobyov, The Fibonacci Numbers, D.C. Heath and Company, Boston 1963
- [2] Tom M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, Heidelberg, Berlin 1976.