Zero-Avoiding Solutions of the Fibonacci Recurrence Modulo a Prime

H. SEDAGHAT

Abstract

There are prime numbers p for which the Fibonacci recurrence $x_{n+1} = x_n + x_{n-1}$ modulo p has solutions that do not visit 0. We identify primes for which such zero-avoiding solutions exist. Further, for such primes we determine the number of all zero-avoiding solutions.

1 Introduction

The many and varied properties of the solutions of the Fibonacci recurrence

$$x_{n+1} = x_n + x_{n-1} \qquad n = 1, 2, 3 \ldots \tag{1}$$

modulo a positive integer are well-known; see, e.g., [1]-[7], [10] and [11]. As is customary, we denote the particular solution of (1) with the initial values $F_0 = 0$, $F_1 = 1$, namely, the Fibonacci sequence by $\{F_n\}$. We consider the general solution of (1) modulo a prime p, i.e., a solution with arbitrary initial values in the field $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z})$.

In modular form $\{F_n\}$ is periodic in $\mathbb{Z}_p$ and its zeroth term is 0 so $\{F_n\}$ visits zero repeatedly. Let the period of $\{F_n\}$ be k_p and let z_p be the first positive index at which F_n is zero; e.g., $k_5 = 20$, $z_5 = 5$ and $k_7 = 16$, $z_7 = 8$. Well-known relations determine z_p if k_p is known; see [2] or Lemma 2 below.

Let a *zero-avoiding* solution of (1) in $\mathbb{Z}_p$ be a solution that does *not* visit 0; i.e., there are initial values x_0, x_1 such that $x_n \not\equiv 0 (\mathrm{mod}\, p)$ for all $n \geq 0$. A solution of (1) may visit 0 even if $x_0, x_1 \neq 0$. Routine calculation shows that (1) has no zero-avoiding solutions in $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_7$ regardless of the initial values. But for the primes 5, 11, 13, 17, 19 zero-avoiding solutions exist in $\mathbb{Z}_p$. These observations raise some natural questions: For which primes p does the Fibonacci recurrence have a zero-avoiding solution in $\mathbb{Z}_p$? For such primes, how abundant are the zero-avoiding solutions? More precisely, *how many* solutions of (1) avoid 0 entirely?

In this paper, primes p for which (1) has zero-avoiding solutions in $\mathbb{Z}_p$ are identified. Where zero-avoiding solutions exist, their number is determined and information about their periods is obtained.

The existence of a zero-avoiding solution has an interesting structural implication for (1). If for some p this difference equation has a solution that avoids 0 in $\mathbb{Z}_p$ then it can be split into a pair of difference equations of order 1. This decomposition is known as a *semiconjugate factorization*, a concept that is defined for both linear and nonlinear difference equations; see [8] for an introduction to this concept. A general study for *linear* difference equations with variable coefficients in rings appears in [9].

2 Zero-avoiding solutions

All additions and multiplications of numbers in $\mathbb{Z}_p$ in this paper are performed modulo p without explicit mention. The collection of all nonzero elements, i.e., the (multiplicative) unit group of $\mathbb{Z}_p$ is denoted G_p. As may be readily verified by induction, the general solution of the second-order difference equation (1) with arbitrary initial values x_0, x_1 may be written as

$$x_n = F_n x_1 + F_{n-1} x_0 \tag{2}$$

If $\{x_n\}$ is an arbitrary solution of (1) in $\mathbb{Z}_p$ then by (2) $x_{k_p} = x_0$ and $x_{k_p+1} = x_1$. It follows that the period of every solution of the Fibonacci recurrence must divide k_p.

Lemma 1 *If $\{x_n\}$ is a zero-avoiding solution of (1) in $\mathbb{Z}_p$ then the period of $\{x_n\}$ divides k_p. Further, for every $u \neq 0$ the sequence $\{x_n u\}$ is also a zero-avoiding solution of (1) with the same period as $\{x_n\}$.*

In the light of Lemma 1 consider a solution $\{x_n\}$ of (1) with $x_0 = 1$ and $x_1 \neq 0$ so that $x_n = F_n x_1 + F_{n-1}$ for $n \geq 1$. Define the subset H_p of G_p as consisting of all initial values x_1 such that $x_n = 0$ for some $n \geq 2$; i.e., H_p is the *set of units that do not generate zero-avoiding solutions* in $\mathbb{Z}_p$.

For $1 \leq n \leq z_p - 1$ setting $x_n = 0$ gives $F_n x_1 + F_{n-1} = 0$ which yields $x_1 = -F_{n-1}/F_n \in G_p$. It follows that for all primes $p \geq 2$,

$$\left\{ -\frac{F_j}{F_{j+1}} : j = 1, 2, \ldots, z_p - 2 \right\} \subset H_p.$$

In fact, it is true that the above set of $z_p - 2$ ratios in G_p is actually equal to H_p. Before proving this and other results, it is convenient to list some known facts from the literature as a lemma. The proofs of these statements may be found in, e.g., [2], [5], [10], [11].

Lemma 2 *(a) k_p is even for all primes $p \geq 3$.*
(b) If $p > 5$ and $p \equiv 1, 4 (\mathrm{mod}\, 5)$, i.e., $p = 10j \pm 1$ for some positive integer j then $k_p | p-1$.
(c) If $p > 5$ and $p \equiv 2, 3 (\mathrm{mod}\, 5)$, i.e., $p = 10j \pm 3$ for some positive integer j then $k_p | 2(p+1)$.
(d) If $p \equiv 2, 3 (\mathrm{mod}\, 5)$ then every solution of (1) has period k_p.
(e) If $k_p = 2(2j+1)$ for some integer $j \geq 0$ then $z_p = k_p$.
(f) If $k_p = 4(2j+1)$ for some integer $j \geq 0$ then $z_p = k_p/4$.
(g) If $k_p = 2^m(2j+1)$ for integers $j \geq 0$ and $m \geq 3$ then $z_p = k_p/2$.
(h) For each prime p, $F_{jz_p+m} = \left(F_{z_p-1}\right)^j F_m$ in $\mathbb{Z}_p$ for all integers $j, m \geq 0$.

Lemma 3 *For every prime $p \geq 2$,*

$$H_p = \left\{ -\frac{F_j}{F_{j+1}} : j = 1, 2, \ldots, z_p - 2 \right\}. \tag{3}$$

Proof. We show that H_p is contained in the above set of ratios. Let $y_1 \in H_p$. Then $y_n = 0$ for a least integer $n \geq 2$. If $n \leq z_p - 1$ then $0 = y_n = F_n y_1 + F_{n-1}$ so $y_1 = -F_{n-1}/F_n$ which is in the set of ratios on the right side in (3). So suppose that $n \geq z_p$. Then there are integers $j \geq 1$

and $m \in \{0, 1, \ldots, z_p - 1\}$ such that $n = jz_p + m$ and by Lemma 2(h), $F_n = \left(F_{z_p-1}\right)^j F_m$. If $m = 0$ then $F_n = 0$ so $y_n = F_{n-1} \neq 0$, a contradiction. Further, if $m = 1$ then $n - 1 = jz_p$ so $F_{n-1} = 0$. This implies that $F_n \neq 0$ so $y_n = F_n y_1 \neq 0$, again a contradiction. Thus $2 \leq m \leq z_p - 1$ and since $\left(F_{z_p-1}\right)^j \not\equiv 0 (\mathrm{mod}\, p)$,

$$y_1 = -\frac{F_{n-1}}{F_n} = -\frac{\left(F_{z_p-1}\right)^j F_{m-1}}{\left(F_{z_p-1}\right)^j F_m} = -\frac{F_{m-1}}{F_m}.$$

Hence, y_1 is in the set on the right hand side of (3) whether $n < z_p$ or $n \geq z_p$ and the proof is complete. ■

Lemma 4 *$H_p = G_p$ if and only if $z_p = p + 1$.*

Proof. By definition, $H_p \subset G_p$ and G_p has $p - 1$ elements. By Lemma 3, H_p has at most $z_p - 2$ elements. If all of these elements are distinct then $H_p = G_p$ if and only if $z_p - 2 = p - 1$; i.e., if and only if $z_p = p + 1$.

To complete the proof it is necessary to show that

$$-\frac{F_i}{F_{i+1}} \neq -\frac{F_j}{F_{j+1}} \tag{4}$$

for all integers i, j such that $1 \leq i < j \leq z_p - 2$. Suppose on the contrary that

$$\frac{F_i}{F_{i+1}} = \frac{F_j}{F_{j+1}}$$

for some pair $i, j \in \{1, \ldots, z_p - 2\}$ with $i < j$. Then

$$\frac{F_{i+1}}{F_i} = \frac{F_{j+1}}{F_j} \Rightarrow \frac{F_i + F_{i-1}}{F_i} = \frac{F_j + F_{j-1}}{F_j} \Rightarrow \frac{F_{i-1}}{F_i} = \frac{F_{j-1}}{F_j}.$$

Reducing the indices may be continued in this way for i steps to yield

$$\frac{F_0}{F_1} = \frac{F_{j-i}}{F_{j-i+1}}$$

which is clearly false. This contradiction establishes (4) and completes the proof. ■

The following is an immediate consequence of Lemmas 2 and 4.

Corollary 5 *(a) If $p \equiv 1, 4 (\mathrm{mod}\, 5)$ or $p = 5$ then the Fibonacci recurrence (1) has a zero-avoiding solution modulo p whose period divides k_p.*

(b) If $p \equiv 2, 3 (\mathrm{mod}\, 5)$ and $z_p < p + 1$ then the Fibonacci recurrence (1) has a zero-avoiding solution modulo p with period k_p.

The condition $z_p < p + 1$ is satisfied in particular for all of the primes less than 2000 that are listed in the table in [11]. The table in [1] contains the values of z_p for primes between 2000 and 3000 which makes it easy to tell which ones possess the zero-avoidance property. A table of zeros for primes between 3000 and 10000 appears in [4].

3 Equivalence classes and eigensequences

If $\{x_n\}$ is a zero-avoiding solution of the Fibonacci recurrence (1) in $\mathbb{Z}_p$ then by Lemma 1 so is the sequence $\{x_n u\}$ for every nonzero $u \in \mathbb{Z}_p$. Let us call two zero-avoiding solutions $\{x_n\}$ and $\{y_n\}$ *equivalent* if $y_n = x_n u$ for all $n \geq 0$ and some nonzero $u \in \mathbb{Z}_p$. This is an equivalence relation in the set of zero-avoiding solutions for a fixed prime p where zero-avoiding solutions exist. Not all zero-avoiding solutions are equivalent; consider the following two zero-avoiding solutions of (1) in $\mathbb{Z}_{29}$

$$1, 6, 7, 13, 20, 4, 24, 28, 23, 22, 16, 9, 25, 5, 1, 6, \ldots$$
$$1, 4, 5, 9, 14, 23, 8, 2, 10, 12, 22, 5, 27, 3, 1, 4, \ldots$$

each of which has period 14. These solutions are not equivalent because the first term is 1 in both cases but the second terms are not equal. We may ask, in what essential sense are these sequences *different*? An answer to this question is found by checking the *ratios* of consecutive terms (mod 29) in each case:

$$\frac{6}{1} = 6,\ \frac{7}{6} = 7(5) = 6,\ \frac{13}{7} = 13(25) = 6,\ \frac{20}{13} = 20(9) = 6, \ldots$$
$$\frac{4}{1} = 4,\ \frac{5}{4} = 5(22) = 23,\ \frac{9}{5} = 9(6) = 25,\ \frac{14}{9} = 14(13) = 8, \ldots$$

To gain a deeper understanding of the zero-avoiding solutions of (1) we now examine the sequences of ratios of their consecutive terms in the multiplicative group G_p. These ratios are subject to greater restrictions and yet, zero-avoiding solutions are easily recovered from them.

Specifically, let $\{x_n\}$ be a zero-avoiding solution of (1) so that $x_n \neq 0$ for all $n \geq 0$. Then the sequence $\{x_n/x_{n-1}\}$ with $x_0 = 1$ is well-defined and

$$\frac{x_{n+1}}{x_n} = \frac{x_n + x_{n-1}}{x_n} = 1 + \frac{x_{n-1}}{x_n}.$$

If $r_n = x_n/x_{n-1}$ then the sequence $\{r_n\}$ satisfies the first-order rational recurrence

$$r_{n+1} = 1 + \frac{1}{r_n} \tag{5}$$

in G_p. Conversely, if a solution $\{r_n\}$ for (5) exists in G_p then a zero-avoiding solution exists for the Fibonacci recurrence (1) with $x_0 = 1$ and $x_n = r_n x_{n-1}$ for $n \geq 1$. Since $r_n \neq 0$ for all n it follows that $x_n \neq 0$ also.

Unlike the solutions of the second-order equation (1), a solution of (5) repeats as soon as $r_n = r_1 = x_1$ for some $n \geq 2$. Thus, each period or cycle of the sequence $\{r_n\}$ *consists of distinct terms in the complement* $G_p \backslash H_p$.

The following lemma answers the question as to whether zero-avoiding solutions having the same sequence of ratios are equivalent. This lemma has the same flavor as the result in calculus which states that two functions having the same derivative are different by at most a constant.

Lemma 6 *Two zero-avoiding solutions of the Fibonacci recurrence (1) are equivalent if and only if they have the same sequence of consecutive ratios.*

Proof. Suppose that $\{x_n\}$ and $\{y_n\}$ are zero-avoiding solutions with the same sequence $\{r_n\}$ of consecutive ratios. Let $u = y_0/x_0$ and note that

$$y_1 = r_1 y_0 = r_1 x_0 u = x_1 u.$$

Now, by straightforward induction $y_n = x_n u$ for all n; i.e., $\{x_n\}$ and $\{y_n\}$ are equivalent. Conversely, assume that $y_n = x_n u$ for all n and some $u \neq 0$ and let $\{r_n\}$ be the sequence of consecutive ratios for $\{x_n\}$. Then for every $n \geq 1$,

$$\frac{y_n}{y_{n-1}} = \frac{x_n u}{x_{n-1} u} = \frac{x_n}{x_{n-1}} = r_n$$

so $\{r_n\}$ is also the sequence of consecutive ratios for $\{y_n\}$. ■

We call the ratios sequence $\{r_n\}$ an *eigensequence* of (1) because a *constant* eigensequence, i.e., a solution of the equation $r = 1+1/r$ or equivalently, a solution of the quadratic $r^2-r-1 = 0$ in G_p is just an eigenvalue of (1).

In this paper we consider eigensequences of a difference equation with constant coefficients but as might be expected *eigensequences are especially relevant to difference equations with variable coefficients.* See [9] for applications of eigensequences to linear difference equations with variable coefficients in rings including, for difference equations with periodic coefficients, conditions that imply the existence of periodic eigensequences of units and thus, semiconjugate factorizations.

Theorem 7 *(a) If $p \equiv 1, 4 (\mathrm{mod}\, 5)$ then each $r \in G_p \backslash H_p$ generates an eigensequence of the Fibonacci recurrence whose period is either 1 (i.e., r is an eigenvalue) or else it has period z_p which divides $p-1$. The total number of eigensequences is $E_p = (p-1)/z_p + 1$. If $p = 5$ then $G_p \backslash H_p = \{3\}$ and the unique eigenvalue 3 is the only eigensequence. If $z_p = p-1$ then the only eigensequences are the two eigenvalues.*

(b) If $p \equiv 2, 3 (\mathrm{mod}\, 5)$ and $z_p < p+1$ for some prime p then each $r \in G_p \backslash H_p$ generates an eigensequence with period z_p which divides $p+1$. The number of eigensequences is $E_p = (p+1)/z_p - 1$. If $z_p = p+1$ then there are no eigensequences in $\mathbb{Z}_p$ for the Fibonacci recurrence.

Proof. (a) By Lemma 2(b) $z_p | p-1$. Also Lemma 4 implies that $G_p \backslash H_p$ is nonempty and by quadratic reciprocity, there are two eigenvalues λ^-, λ^+ in $G_p \backslash H_p$. Removing these from $G_p \backslash H_p$ leaves the set $S = G_p \backslash (H_p \cup \{\lambda^-, \lambda^+\})$ which contains $p-1-z_p$ elements. If $z_p = p-1$ then we are done. Otherwise, $r = r_1 \in S$ generates a non-constant eigensequence $\{r_n\}$ whose period must be z_p. To see this, note that by (2), $x_n = F_n x_1 + F_{n-1}$ for $n \geq 1$ with $x_0 = 1$ and $x_1 = r_1 x_0 = r_1$. Therefore, if m is the period of $\{r_n\}$ then

$$r_1 = r_{m+1} = \frac{x_{m+1}}{x_m} = \frac{F_{m+1} r_1 + F_m}{F_m r_1 + F_{m-1}}$$

The above equality can be rearranged as

$$0 = F_m r_1^2 + (F_{m-1} - F_{m+1}) r_1 - F_m = (r_1^2 - r_1 - 1) F_m.$$

Since r_1 is not an eigenvalue it follows that $F_m = 0$, i.e., $z_p \leq m$. Further, $m \leq z_p$ because

$$r_{z_p+1} = \frac{F_{z_p+1} r_1 + F_{z_p}}{F_{z_p} r_1 + F_{z_p-1}} = \frac{F_{z_p-1} r_1}{F_{z_p-1}} = r_1.$$

Therefore, $m = z_p$ as claimed. Thus, all (non-constant) eigensequences have the same period z_p and they are all contained in the set S. If E'_p is the number of these eigensequences then $z_p E'_p$ equals the number of elements in S, i.e.,

$$z_p E'_p = p - 1 - z_p, \text{ or } \quad E'_p = \frac{p-1}{z_p} - 1.$$

Now adding in the two eigenvalues λ^-, λ^+ and denoting the total number of eigensequences (constant and non-constant) by E_p we obtain $E_p = (p-1)/z_p + 1$, as claimed. The assertion about $p = 5$ has already been verified in the previous discussion above.

(b) By Lemma 2(c) $z_p | 2(p+1)$. Since $p+1$ is even, by Lemma 2(f),(g) $z_p \leq p+1$. If $z_p = p+1$ then Lemma 4 implies that $G_p = H_p$ and there are no eigensequences. If $z_p < p+1$ then $G_p \backslash H_p$ is nonempty again by Lemma 4. There are no eigenvalues in $G_p \backslash H_p$ since 5 is not a square in this case. Next, as in (a), the eigensequences in $G_p \backslash H_p$ all have period z_p so if their number is E_p then $z_p E_p$ is the number of elements in $G_p \backslash H_p$, i.e., $p + 1 - z_p$. This gives

$$E_p = \frac{p+1}{z_p} - 1$$

and completes the proof. ■

Since there are $p-1$ nonzero terms in $\mathbb{Z}_p$, Lemmas 1 and 6 imply that the number of zero-avoiding solutions in $\mathbb{Z}_p$ is $(p-1)E_p$. Hence Theorem 7 readily implies the following.

Corollary 8 *(a) If $p \equiv 1, 4 (\mathrm{mod}\, 5)$ then there are $(p-1)^2/z_p + p - 1$ zero-avoiding solutions of the Fibonacci recurrence in $\mathbb{Z}_p$. Also, there are four zero-avoiding solutions in $\mathbb{Z}_5$.*

(b) If $p \equiv 2, 3 (\mathrm{mod}\, 5)$ then there are $(p^2-1)/z_p - p + 1$ zero-avoiding solutions of the Fibonacci recurrence in $\mathbb{Z}_p$.

The table below lists the number E_p of eigensequences (including eigenvalues, where they exist) of the Fibonacci recurrence in $\mathbb{Z}_p$ for all primes less than 100. From this table we may infer, for instance, that for $p = 61$ there are 5 eigensequences (equivalence classes of zero-avoiding solutions) of which two are constants (eigenvalues) and the other three are sequences of period 15 each.

p	2	3	5	7	11	13	17	19	23	29	31	37	41
z_p	3	4	5	8	10	7	9	18	24	14	30	19	20
E_p	0	0	1	0	2	1	1	2	0	3	2	1	3
-	-	-	-	-	-	-	-	-	-	-	-	-	-
p	43	47	53	59	61	67	71	73	79	83	89	97	
z_p	44	16	27	58	15	68	70	37	78	84	11	49	
E_p	0	2	1	2	5	0	2	1	2	0	9	1	

TABLE 1. Zeros and Eigensequences

4 Two related problems

An extension of the results in the preceding sections to finite rings of type $\mathbb{Z}_m$ may be considered, where m is a positive integer. In this setting eigensequences correspond to zero-*divisor*-avoiding sequences, or more precisely, sequences of units. Some reflection and experimentation suggest that the following may be true:

Conjecture: *The Fibonacci recurrence (1) has an eigensequence in $\mathbb{Z}_m$ if and only if $m \not\equiv 0 (\mathrm{mod}\, p)$ for all primes p where $z_p = p + 1$.*

Since the condition $z_p = p + 1$ applies only to primes of type $p \equiv 2, 3 (\mathrm{mod}\, 5)$, if the conjecture is true then eigensequences exist in $\mathbb{Z}_m$ when, in particular, all of the prime factors of m are of type $p \equiv 0, 1, 4 (\mathrm{mod}\, 5)$. The smallest composite integer that satisfies the conditions of the conjecture is $m = 25$ and indeed, $\mathbb{Z}_{25}$ contains the following eigensequence with period 5

$$3, 18, 8, 23, 13, 3, \ldots$$

On the other hand, routine arguments show that rings $\mathbb{Z}_{2j}$ and $\mathbb{Z}_{3j}$ contain no eigensequences of (1) for every positive integer j. In such rings, every solution of the Fibonacci recurrence contains zero divisors.

Going in a different direction, there is the inverted problem of identifying all primes p for which a particular solution of the Fibonacci recurrence modulo p, e.g., the sequence $\{L_n\}$ of Lucas numbers ($L_0 = 2$, $L_1 = 1$) is zero-avoiding. These primes must satisfy the hypotheses of Theorem 7 which yield necessary conditions for $\{L_n\}$ to be zero-avoiding. These conditions are not sufficient though; for $p = 29, 47$ in the above list of Zeros and Eigensequences we find that $L_{10} \equiv 0 (\mathrm{mod}\, 29)$, $L_8 \equiv 0 (\mathrm{mod}\, 47)$. Using the same table and straightforward calculations we find that $\{L_n\}$ is zero-avoiding modulo the following primes less than 100

$$5, 13, 17, 37, 53, 61, 73, 89, 97.$$

Further, in [1] we count 49 prime numbers between 2000 and 3000 for which Lucas sequences are zero-avoiding.

References

[1] U. Alfred, Additional factors of the Fibonacci and Lucas series, *Fibonacci Quarterly* **1** (1963):34-42.

[2] U. Alfred, Relation of zeros to periods in the Fibonacci sequence modulo a prime, *The American Mathematical Monthly* **71** (1964):897-99.

[3] A. Andreassian, Fibonacci sequences modulo m, *Fibonacci Quarterly* **12** (1974):51-54.

[4] R.P. Backstrom, On the determination of the zeros of the Fibonacci sequence, *Fibonacci Quarterly* **4** (1966):313-22.

[5] S. Gupta, P. Rockstroh, F.E. Su, Splitting fields and periods of Fibonacci sequences modulo primes, *The Mathematics Magazine* **85** (2012):130-35.

[6] S.E. Mamangakis, Remarks on the Fibonacci series modulo m, *The American Mathematical Monthly* **68** (1961):648–49..

[7] D.W. Robinson, The Fibonacci matrix modulo m, *Fibonacci Quarterly* **1** (1963):29-36.

[8] H. Sedaghat, *Form Symmetries and Reduction of Order in Difference Equations*, Chapman & Hall/CRC Press, Boca Raton (2011).

[9] H. Sedaghat, Semiconjugate factorizations of higher order linear difference equations in rings, submitted; preprint 1301.2804 available on arXiv.org.

[10] J. Vinson, The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence, *Fibonacci Quarterly* **1** (1963):37-46.

[11] D.D. Wall, Fibonacci series modulo m, *The American Mathematical Monthly* **67** (1960):525-32.

Department of Mathematics, Virginia Commonwealth University
Richmond, Virginia, 23284-2014, USA; h.sedaghat@discretedynamics.net