POWER FIBONACCI SEQUENCES

JOSHUA IDE AND MARC S. RENAULT

Abstract. We examine integer sequences G satisfying the Fibonacci recurrence relation $G_n = G_{n-1} + G_{n-2}$ that also have the property that $G \equiv 1, a, a^2, a^3, \ldots \pmod{m}$ for some modulus m. We determine those moduli m for which these power Fibonacci sequences exist and the number of such sequences for a given m. We also provide formulas for the periods of these sequences, based on the period of the Fibonacci sequence F modulo m. Finally, we establish certain sequence/subsequence relationships between power Fibonacci sequences.

1. Introduction

Let G be a bi-infinite integer sequence satisfying the recurrence relation $G_n = G_{n-1} + G_{n-2}$. If $G \equiv 1, a, a^2, a^3, \ldots \pmod{m}$ for some modulus m, then we will call G a *power Fibonacci sequence modulo* m.

Example 1.1. *Modulo* $m = 11$*, there are two power Fibonacci sequences:*

$$1, 8, 9, 6, 4, 10, 3, 2, 5, 7, 1, 8 \ldots \text{ and } 1, 4, 5, 9, 3, 1, 4, \ldots$$

Curiously, the second is a subsequence of the first. For modulo 5 *there is only one such sequence* $(1, 3, 4, 2, 1, 3, \ldots)$*, for modulo* 10 *there are no such sequences, and for modulo* 209 *there are four of these sequences.*

In the next section, Theorem 2.1 will demonstrate that $209 = 11 \cdot 19$ is the smallest modulus with more than two power Fibonacci sequences.

In this note we will determine those moduli for which power Fibonacci sequences exist, and how many power Fibonacci sequences there are for a given modulus. We also establish facts on periods of these sequences and show certain sequence/subsequence relationships between these sequences.

2. The Number of Power Fibonacci Sequences, Modulo M

Theorem 2.1. *There is exactly one power Fibonacci sequence modulo* 5*. For* $m \neq 5$*, there exist power Fibonacci sequences modulo* m *precisely when* m *has prime factorization* $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ *or* $m = 5p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$*, where each* $p_i \equiv \pm 1 \pmod{10}$*; in either case there are exactly* 2^k *power Fibonacci sequences modulo* m*.*

Proof. $1, a, a^2, \ldots$ is a power Fibonacci sequence modulo m if and only if a is a root of $f(x) = x^2 - x - 1$ modulo m. The roots of $f(x)$ are those residues of the form $2^{-1}(1 + r)$ where $r^2 \equiv 5 \pmod{m}$; necessarily, m is odd. Let $g(x) = x^2 - 5$. Counting the number of solutions to $g(x) \equiv 0 \pmod{m}$ for odd m thus determines the number of power Fibonacci sequences mod m.

Correspondence should be sent to Marc Renault msrenault@ship.edu.

This paper appears in *The Fibonacci Quarterly*, vol. 50, no. 2, May 2012. pp. 175 – 180 .

By inspection, the only solution to $x^2 \equiv 5 \pmod 5$ is 0, and there are no solutions to $x^2 \equiv 5 \pmod{25}$. Consequently, $x^2 \equiv 5 \pmod{5^e}$ has a solution only when $e = 1$, and that solution is $x \equiv 0 \pmod 5$. The corresponding power Fibonacci sequence is $1, 3, 4, 2, 1, 3, \ldots$.

Consider now the roots of $g(x) \pmod p$ for an odd prime $p \neq 5$. By use of the law of quadratic reciprocity [2,3], one finds that 5 is a quadratic residue modulo primes p of the form $p \equiv \pm 1 \pmod{10}$ and 5 is a quadratic nonresidue for $p \equiv \pm 3 \pmod{10}$. See, e.g., [4, Lem. 3.9]. Thus, if $p \equiv \pm 1 \pmod{10}$ then $g(x) \pmod p$ has two distinct roots.

Now that we know existence and number of roots of $g(x) \pmod p$, we address the existence and number of roots of $g(x) \pmod{p^e}$ for positive integers e. Hensel's Lemma is a useful tool here (see, e.g., [3, Thm. 2.23] or [2, §4.3]). It states that if $h(x)$ is an integer polynomial with root $a \pmod{p^i}$, and if $h'(a) \not\equiv 0 \pmod p$, then $h(x)$ has a root $\bar{a} \pmod{p^{i+1}}$ with the property that $\bar{a} \equiv a \pmod{p^i}$; in essence, distinct roots of $h(x) \pmod{p^i}$ "lift" to distinct roots of $h(x) \pmod{p^{i+1}}$. With $g(x) = x^2 - 5$, and p a prime of the form $p \equiv \pm 1 \pmod{10}$, we find that if x_0 is a root of $g(x) \pmod p$, then $g'(x_0) = 2x_0 \not\equiv 0 \pmod p$. By Hensel's Lemma it follows that $g(x) \pmod{p^e}$ has two distinct roots for every positive integer e.

Lastly, we turn to composite moduli and make use of the Chinese Remainder Theorem from elementary number theory [2,3]. If m and n are relatively prime, if $g(x) \equiv 0 \pmod m$ has s solutions, and if $g(x) \equiv 0 \pmod n$ has t solutions, then $g(x) \equiv 0 \pmod{mn}$ has st solutions. The statement of the theorem now follows. □

3. The Periods of Power Fibonacci Sequences

Let $\pi(m)$ denote the period of the Fibonacci sequence $F = 0, 1, 1, 2, 3, \ldots$ modulo m. There is no known explicit formula for $\pi(m)$, however, it turns out [6] that if $(m, n) = 1$ then $\pi(mn) = [\pi(m), \pi(n)]$ — this is not difficult to see, for if S is *any* periodic sequence mod mn and $(m, n) = 1$, then its period is the least common multiple of the period of S taken mod m and the period of S taken mod n. For $m > 2$ it is known that $\pi(m)$ is even (due to Wall [6, Thm. 4]; see [4, Thm. 3.1] for a simpler proof). Also, for any integer sequence G satisfying the Fibonacci recurrence relation $G_n = G_{n-1} + G_{n-2}$, it is known that the period of G mod m divides $\pi(m)$ [6]. The main result in this section, Theorem 3.3, establishes a relationship between $\pi(m)$ and the period of power Fibonacci sequences mod m.

Although there is no known formula for $\pi(m)$, the interested reader should refer to [5] and [1] for discussions on computing $\pi(m)$.

If r is a square root of 5 modulo m, then $2^{-1}(1 + r)$ and $2^{-1}(1 - r)$ are conjugate roots of $f(x) = x^2 - x - 1 \pmod m$, and the product of these roots is congruent to -1 mod m. If $(a, m) = 1$, then the order of a modulo m is the least positive integer i such that $a^i \equiv 1 \pmod m$. We will denote the order of a modulo m by $|a|_m$ or often, if the context is clear, simply by $|a|$ (not the absolute value of a!). Observe that if a is a root of $f(x) \pmod m$, then $|a|$ is exactly the period of the power Fibonacci sequence $1, a, a^2, \ldots$ modulo m.

We first dispose with a technical lemma which will be useful in a couple proofs to follow.

Lemma 3.1. *Let p be an odd prime and let e be a positive integer. If $x^2 \equiv 1 \pmod{p^e}$ then $x \equiv \pm 1 \pmod{p^e}$.*

Proof. If $x^2 \equiv 1 \pmod{p^e}$, then $(x + 1)(x - 1) \equiv 0 \pmod{p^e}$. If $p|(x + 1)$ and $p|(x - 1)$, then $p|2$; but this is a contradiction since p is odd. Thus, either $x + 1 \equiv 0 \pmod{p^e}$ or $x - 1 \equiv 0 \pmod{p^e}$. □

The main result of this section, Theorem 3.3, is largely a proof by induction, and the following lemma establishes a base case for the induction.

Lemma 3.2. *Let p be a prime of the form $p \equiv \pm 1 \pmod{10}$, and let α and β be the two roots of $f(x) = x^2 - x - 1 \pmod{p^e}$. Without loss of generality, assume $|\alpha| \geq |\beta|$.*

(a) If $\pi(p^e) \equiv 0 \pmod 4$, then $|\alpha| = |\beta| = \pi(p^e)$.
(b) If $\pi(p^e) \equiv 2 \pmod 4$, then $|\alpha| = 2|\beta| = \pi(p^e)$.

Proof. Our key observation is that $\alpha\beta \equiv -1$, and so

$$\alpha^n \beta^n \equiv (-1)^n \pmod{p^e}$$

for any n. Now if $|\alpha| = |\beta| = n$, then $1 \equiv \alpha^n\beta^n \equiv (-1)^n$ and so n must be even. Since n is even and p is odd, Lemma 3.1 implies $\alpha^{n/2} \equiv \beta^{n/2} \equiv -1 \pmod{p^e}$. Thus $(-1)^{n/2} \equiv \alpha^{n/2}\beta^{n/2} \equiv (-1)(-1) \equiv 1 \pmod{p^e}$. Consequently, $n/2$ is even and we find $4|n$.

On the other hand, if $|\alpha| > |\beta| = n$, then $\alpha^n \equiv (-1)^n$. First we see that $n = |\beta|$ must be odd. Moreover, $\alpha^{2n} \equiv 1$, so $|\alpha|$ divides $2n$. Since $|\alpha| > n$, we conclude that $|\alpha| = 2n$.

Finally, one can confirm Binet's formula, that terms of the Fibonacci sequence modulo p^e are given by $F_n \equiv (\alpha - \beta)^{-1}(\alpha^n - \beta^n)$. Thus, $\pi(m) \leq [|\alpha|, |\beta|] = |\alpha|$. Since the period of any integer Fibonacci sequence modulo m divides $\pi(m)$, we must conclude that $|\alpha| = \pi(p^e)$. □

We are now ready to state our main result on the periods of power Fibonacci sequences.

Theorem 3.3. *Let $m = p_1^{e_1} \cdots p_k^{e_k}$, a product of primes of the form $p_i \equiv \pm 1 \pmod{10}$.*

(a) If $\pi(m) \equiv 0 \pmod 4$, then modulo m, every power Fibonacci sequence has period $\pi(m)$.
(b) If $\pi(m) \equiv 2 \pmod 4$, then modulo m, one power Fibonacci sequence has (odd) period $\frac{1}{2}\pi(m)$ and all the others have period $\pi(m)$.
(c) If $\pi(m) \equiv 0 \pmod 4$, then modulo $5m$, every power Fibonacci sequence has period $\pi(m)$.
(d) If $\pi(m) \equiv 2 \pmod 4$, then modulo $5m$, every power Fibonacci sequence has period $2\pi(m)$.

Proof. For parts (a) and (b) we wish to compute the periods of the power Fibonacci sequences modulo m. We begin by observing that these parts are satisfied for $m = p^e$ by Lemma 3.2. Now let m and n be relatively prime, and for induction, assume that the theorem holds modulo m and n. We will show that it is true modulo mn as well, and this will prove parts (a) and (b).

Denote the roots of $f(x) = x^2 - x - 1 \pmod m$ by $a_1, a_2, \ldots, a_s$, and denote the roots of $f(x) \pmod n$ by $b_1, b_2, \ldots, b_t$. Then the st roots of $f(x) \pmod{mn}$ can be denoted c_{ij} for $1 \leq i \leq s$ and $1 \leq j \leq t$ with root c_{ij} satisfying the simultaneous congruences

$$\begin{aligned} c_{ij} &\equiv a_i \pmod m \\ c_{ij} &\equiv b_j \pmod n . \end{aligned}$$

One sees that $|c_{ij}|_{mn} = [|a_i|_m, |b_j|_n]$.

To establish part (a) of the theorem, suppose that either $\pi(m) \equiv 0 \pmod 4$ or $\pi(n) \equiv 0 \pmod 4$. Then $|c_{ij}|_{mn} = [\pi(m), \pi(n)]$ or $[\pi(m), \frac{1}{2}\pi(n)]$ or $[\frac{1}{2}\pi(m), \pi(n)]$, but in all cases we find that $|c_{ij}|_{mn} = \pi(mn) \equiv 0 \pmod 4$.

To establish part (b) of the theorem, suppose that $\pi(m) \equiv 2 \pmod 4$ and $\pi(n) \equiv 2 \pmod 4$. If $|c_{ij}|_{mn} = [\pi(m), \pi(n)]$ or $[\pi(m), \frac{1}{2}\pi(n)]$ or $[\frac{1}{2}\pi(m), \pi(n)]$, then in these cases we have $|c_{ij}|_{mn} = \pi(mn) \equiv 2 \pmod 4$. The one remaining case is $|c_{ij}|_{mn} = [\frac{1}{2}\pi(m), \frac{1}{2}\pi(n)] = \frac{1}{2}\pi(mn)$, which is odd. This final case occurs only if a_i is that single root of odd order modulo m and b_j is that single root of odd order modulo n.

For parts (c) and (d) we wish to compute the periods of the power Fibonacci sequences modulo $5m$. Once again, label the roots of $f(x) = x^2 - x - 1 \pmod m$ by $a_1, a_2, \ldots, a_s$, and

observe that the only root of $f(x)$ mod 5 is the residue 3. Now the roots of $f(x)$ mod $5m$ can be denoted c_i where

$$\begin{aligned} c_i &\equiv 3 \pmod 5 \\ c_i &\equiv a_i \pmod m . \end{aligned}$$

Now $|c_i|_{5m} = [|3|_5, |a_i|_m] = [4, |a_i|_m]$. If $\pi(m) \equiv 0 \pmod 4$, then $|a_i|_m = \pi(m) \equiv 0 \pmod 4$. Thus $|c_i|_{5m} = [4, \pi(m)] = \pi(m)$, and (c) is proved.

Lastly, for part (d), if $\pi(m) \equiv 2 \pmod 4$, then either $|a_i|_m = \pi(m) \equiv 2 \pmod 4$ or $|a_i|_m = \frac{1}{2}\pi(m) \equiv 1 \pmod 2$. In the first case, $|c_i|_{5m} = [4, \pi(m)] = 2\pi(m)$, and in the second case $|c_i|_{5m} = [4, \frac{1}{2}\pi(m)] = 2\pi(m)$. □

4. Subsequence Relationships Among Power Fibonacci Sequences

Theorem 4.1. *Let α and β be conjugate roots of $x^2 - x - 1 \pmod m$. Assume $|\alpha| \geq |\beta|$, let $A = 1, \alpha, \alpha^2, \ldots$, and let $B = 1, \beta, \beta^2, \ldots$.*

(a) If $|\alpha| > |\beta|$, then B is a subsequence of A.
(b) If $|\alpha| = |\beta|$ and $m = p^e$ for a prime $p \equiv \pm 1 \pmod{10}$, then A and B are subsequences of each other.

Proof. Assume the hypotheses of the theorem, and let $2n = |\alpha|$. As a first step we make the following claim:

If $\alpha^n \equiv -1 \pmod m$, then B is a subsequence of A.

The truth of the claim can be seen by first multiplying the congruence by α^{-1} to get $\alpha^{n-1} \equiv -\alpha^{-1}$. Of course, since $\alpha\beta \equiv -1 \pmod m$, we have $-\alpha^{-1} \equiv \beta$, and so we find that $\alpha^{n-1} \equiv \beta$. Consequently, B is a subsequence of A.

For part (a) of the theorem, assume $|\alpha| > |\beta|$. By Theorem 3.3, $|\alpha| = 2|\beta| = 2n$ and n is odd. Then $\alpha\beta \equiv -1$ implies $(\alpha\beta)^n \equiv (-1)^n$, and since $\beta^n \equiv 1$, we get $\alpha^n \equiv -1$. By the claim above, we deduce B is a subsequence of A.

For part (b), first observe that $(\alpha^n)^2 = \alpha^{2n} \equiv 1 \pmod{p^e}$. Lemma 3.1 now implies that $\alpha^n \equiv -1 \pmod{p^e}$, and again, by the claim at the beginning of the proof, we conclude B is a subsequence of A. Since $|\alpha| = |\beta|$, we may switch the roles of α and β and with the same proof also conclude that A is a subsequence of B. □

We conclude with some examples that show that Theorem 4.1 is "complete."

Can more be said regarding part (b) of the theorem for a modulus m that is not a power of a prime? If $m = 209 = 11 \cdot 19$, then $\alpha = 195$ and $\beta = 15$ are conjugate roots with $|195| = |15| = 90$. Computations show us that A and B have 45 terms in common, so they cannot be subsequences of each other. On the other hand, if $m = 305 = 5 \cdot 61$, then $\alpha = 288$ and $\beta = 18$ are conjugate roots with $|288| = |18| = 60$. In this case, computations show that A and B are subsequences of each other.

What of the situation where α and β are both roots of $x^2 - x - 1 \pmod m$, but they are not conjugate roots? It is very often the case that B is not a subsequence of A, but sometimes it still can happen that B is a subsequence of A. For example, consider again the case $m = 209 = 11 \cdot 19$. Then $x^2 - x - 1 \pmod{209}$ has four roots: 15, 81, 129, 195. The conjugate pairs are $(195, 15)$ and $(129, 81)$, and $|195| = |15| = |129| = 90$, whereas $|81| = 45$. If we choose $\alpha = 15$ and $\beta = 81$, then B is not a subsequence of A. However, if $\alpha = 195$ and $\beta = 81$, then it turns out that B is a subsequence of A.

Acknowledgment

The authors wish to express their appreciation to an anonymous referee for the careful reading and the helpful comments and suggestions that improved the quality of this paper.

References

[1] D. L. Herrick, *On the periodicity of the terminal digits in the Fibonacci sequence*, The Fibonacci Quarterly, **11** (1973), 535–538.
[2] G. Jones and J. Jones, *Elementary Number Theory*, Springer, 1998.
[3] I. Niven, H. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc., 1991.
[4] M. S. Renault, *The Fibonacci sequence under various moduli*, Master's Thesis, Wake Forest University, 1996. Available at `http://webspace.ship.edu/msrenault/fibonacci/FibThesis.pdf`.
[5] J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, The Fibonacci Quarterly, **1** (1963), 37–48.
[6] D. D. Wall, *Fibonacci series modulo m*, The American Mathematical Monthly, **67** (1960), 525–532.

MSC2010: 11B39, 11B50, 11A07

Department of Mathematics, Shippensburg University, Pennsylvania, USA
E-mail address: `ji1574@ship.edu`

Department of Mathematics, Shippensburg University, Pennsylvania, USA
E-mail address: `msrenault@ship.edu`