involve
a journal of mathematics

The Fibonacci sequence under a modulus: computing all moduli that produce a given period

Alex Dishong and Marc S. Renault

msp

2018 vol. 11, no. 5

INVOLVE 11:5 (2018)
dx.doi.org/10.2140/involve.2018.11.769

The Fibonacci sequence under a modulus: computing all moduli that produce a given period

Alex Dishong and Marc S. Renault

(Communicated by Kenneth S. Berenhaut)

The Fibonacci sequence $F = 0, 1, 1, 2, 3, 5, 8, 13, \ldots$, when reduced modulo m is periodic. For example, $F \bmod 4 = 0, 1, 1, 2, 3, 1, 0, 1, 1, 2, \ldots$. The period of $F \bmod m$ is denoted by $\pi(m)$, so $\pi(4) = 6$. In this paper we present an algorithm that, given a period k, produces all m such that $\pi(m) = k$. For efficiency, the algorithm employs key ideas from a 1963 paper by John Vinson on the period of the Fibonacci sequence. We present output from the algorithm and discuss the results.

1. The problem

Consider the usual Fibonacci sequence $F = 0, 1, 1, 2, 3, 5, 8, \ldots$, with $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$. When reduced modulo m, the Fibonacci sequence is periodic. For example, $F \bmod 4 = 0, 1, 1, 2, 3, 1, 0, 1, 1, \ldots$. The period of $F \bmod m$ is denoted by $\pi(m)$, so we see that $\pi(4) = 6$. The properties of $\pi(m)$ have been studied extensively; see, e.g., [Gupta et al. 2012; Robinson 1963; Vinson 1963; Wall 1960]. One might ask, of course, if there are any other values of m such that $\pi(m) = 6$. The answer is no (you can verify this by hand), but it turns out that there are 10 different moduli m such that $\pi(m) = 24$ (namely, 6, 9, 12, 16, 18, 24, 36, 48, 72, 144). Our goal is to construct an efficient algorithm that, given a period k, produces all m such that $\pi(m) = k$.

It is instructive to first consider how one might solve the problem by brute force. If $\pi(m) = k$, then $F_k \equiv 0 \pmod m$ and $F_{k+1} \equiv 1 \pmod m$. That is, m divides both F_k and $F_{k+1} - 1$. For brute force, we fix k, find all common divisors of F_k and $F_{k+1} - 1$, and then apply the π function to these divisors to see which ones produce the desired value of k. Computing $\pi(m)$ is not difficult but it requires factoring m as a product of primes, then factoring $p \pm 1$ for each prime p that divides m. See [Wall 1960] for theorems on $\pi(m)$ and [Flanagan et al. 2015] for an algorithm for $\pi(m)$ (as well as many other facts about the Fibonacci sequence under a modulus).

MSC2010: primary 11B39, 11B50; secondary 11Y55.
Keywords: Fibonacci sequence, period, algorithm.

By employing key ideas from a 1963 paper by John Vinson on the period of the Fibonacci sequence, we were able to produce an algorithm that does not require computing $\pi(m)$. Instead, the moduli we seek can be produced with simple divisibility tests.

2. The algorithm

In this section we present Theorem 2.1 on which our algorithm is based, pseudocode for the algorithm, and some output. In the next section we provide a proof of Theorem 2.1.

First, we note that $\pi(2) = 3$ but it is known that for $m > 2$, $\pi(m)$ must be even. By inspecting a few small cases, it is easy to see that no moduli produce a period of 4, and the smallest even period is 6. Let $L = 2, 1, 3, 4, 7, \ldots$ denote the Lucas sequence: $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$. It is well-known that $L_n = F_{2n}/F_n = F_{n-1} + F_{n+1}$.

Theorem 2.1. *Given any even $k \geq 6$:*

(1) *If $k \equiv 2 \pmod 4$, then $\pi(m) = k$ if and only if $m \mid L_{k/2}$, and $m \nmid F_q$ for all q such that $q \mid k$ and $q \neq k$.*

(2) *If $k \equiv 4 \pmod 8$, then $\pi(m) = k$ if and only if $m \mid F_{k/2}$, and $m \nmid L_{k/4}$, and $m \nmid F_q$ for all q such that $q \mid \frac{k}{2}$ and $q \neq \frac{k}{2}$ or $\frac{k}{4}$.*

(3) *If $k \equiv 0 \pmod 8$, then $\pi(m) = k$ if and only if $m \mid F_{k/2}$, and $m \nmid F_q$ for all q such that $q \mid \frac{k}{2}$ and $q \neq \frac{k}{2}$.*

The algorithm follows immediately from the theorem.

Algorithm 2.2. Given an integer $k \geq 2$, to produce the set of all m such that $\pi(m) = k$:

Input: an integer $k \geq 2$
If $k = 3$, then return $\{2\}$.
If $k \in \{2, 4\}$ or if k is odd, then return $\{\}$.
If $k \bmod 4 = 2$:
  Let $\mathcal{M} = \{m : m \mid L_{k/2}\}$.
  Let $\mathcal{F} = \{F_q : q \mid k$ and $q \neq k\}$.
If $k \bmod 8 = 4$:
  Let $\mathcal{M} = \{m : m \mid F_{k/2}$ and $m \nmid L_{k/4}\}$.
  Let $\mathcal{F} = \left\{F_q : q \mid \frac{k}{2}\right.$ and $q \neq \frac{k}{2}$ and $\left.q \neq \frac{k}{4}\right\}$.
If $k \bmod 8 = 0$:
  Let $\mathcal{M} = \{m : m \mid F_{k/2}\}$.
  Let $\mathcal{F} = \left\{F_q : q \mid \frac{k}{2}\right.$ and $\left.q \neq \frac{k}{2}\right\}$.
Return $\{m \in \mathcal{M} : m \nmid f$ for all $f \in \mathcal{F}\}$

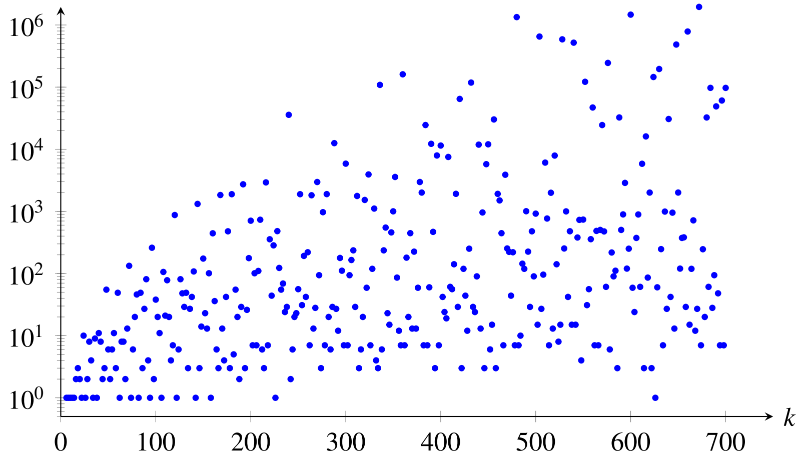

Figure 1. The number of m such that $\pi(m) = k$ for a given k.

Figure 1 shows the results when the algorithm is run on all even k from 6 to 700 and the size of the output set is calculated. The value of k appears on the horizontal axis, and the number of moduli m such that $\pi(m) = k$ is expressed on the vertical axis.

What surprised us most in this study was the incredible number of moduli that can produce a given period. For example, $\pi(m) = 600$ for 1,466,812 different values of m.

Moreover, the algorithm above has much greater speed than simple brute force. When we computed the moduli for all even periods k from 6 to 300, the brute force algorithm took 180.28 seconds, whereas Algorithm 2.2 completed the task in 0.62 seconds. We used the online Sage computer algebra system for our computations [Stein et al. 2016].

3. Proof of Theorem 2.1

The zeros in $F \bmod m$ are evenly spaced. For example, consider $F \bmod 5$:

$$F \bmod 5 = 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, \ldots.$$

(To see why the zeros are evenly spaced, we can use the identities

$$F_{s+t} = F_{s-1}F_t + F_s F_{t+1},$$
$$F_{s-t} = (-1)^t(F_s F_{t+1} - F_{s+1}F_t).$$

If $F_s \equiv F_t \equiv 0$, then $F_{s+t} \equiv 0$ and $F_{s-t} \equiv 0$.)

The *rank* of $F \bmod m$, denoted by $\alpha(m)$, is the least index $i > 0$ such that $F_i \equiv 0 \pmod{m}$. We can deduce, for example, that if $m \mid F_i$, then $\alpha(m) \mid i$. The *order* of F mod m, denoted by $\omega(m)$, is $\pi(m)/\alpha(m)$ (which is an integer since the zeros are evenly spaced). We see above that $\pi(5) = 20$, $\alpha(5) = 5$, and $\omega(5) = 4$.

It turns out that $\pi(2) = 3$, but for all $m > 2$, $\pi(m)$ must be even. As we see in the mod 5 example, $\alpha(m)$ need not be even. It is a remarkable fact that for any m, $\omega(m) = 1$, 2, or 4; this is proven in [Vinson 1963]. In that paper, Vinson studies the relationship between the period, rank, and order. Based on the Vinson paper, Renault was able find several other consequences, and the following theorem is a direct result of Theorem 3.35 and Corollary 3.38 in [Renault 1996].

Theorem 3.1. *For any modulus $m > 2$:*

(1) $\pi(m) \equiv 2 \pmod 4$ *if and only if* $\omega(m) = 1$. *In this case*, $\alpha(m) \equiv 2 \pmod 4$.

(2) *If* $\pi(m) \equiv 4 \pmod 8$, *then* $\omega(m) = 2$ *or* 4. *In this case*, $\alpha(m) \equiv 2 \pmod 4$ *or* $\alpha(m)$ *is odd*, *respectively.*

(3) *If* $\pi(m) \equiv 0 \pmod 8$, *then* $\omega(m) = 2$. *In this case*, $\alpha(m) \equiv 0 \pmod 4$.

Since $\pi(m)$ is even for $m > 2$, the above theorem describes all possible cases for $\pi(m)$. Also, even though the "in this case" portions follow obviously from their preceding statements, we can use them to draw conclusions. For example, we can see from the theorem that $\alpha(m) \equiv 0 \pmod 4$ if *and only if* $\pi(m) \equiv 0 \pmod 8$. We proceed now to the proof of Theorem 2.1.

Proof of Theorem 2.1(1). ($\Rightarrow$) Assume $k \equiv 2 \pmod 4$ and $\pi(m) = k$. Since $k \equiv 2 \pmod 4$, Theorem 3.1 tells us that $\omega(m) = 1$. Thus, $m \nmid F_q$ for all q such that $1 \le q < k$. In particular, $m \nmid F_q$ for any q such that $q \mid k$ and $q \ne k$.

It remains to show that $m \mid L_{k/2}$. By the fact that $\pi(m) = k$ and the identity $F_{-n} = (-1)^{n+1} F_n$, we see that $F_{k-n} \equiv F_{-n} \equiv (-1)^{n+1} F_n \pmod m$. Then, since $\frac{k}{2}$ is odd,

$$F_{k/2-1} = F_{k-(k/2+1)} \equiv -F_{k/2+1} \pmod m.$$

Consequently, $m \mid F_{k/2-1} + F_{k/2+1}$. But by the identity $L_n = F_{n-1} + F_{n+1}$, this is exactly $m \mid L_{k/2}$, as required.

($\Leftarrow$) Assume $k \equiv 2 \pmod 4$ and (a) $m \mid L_{k/2}$ and (b) $m \nmid F_q$ for any q such that $q \mid k$ and $q \ne k$. We must show that $\pi(m) = k$.

By (a), $m \mid F_k$, so $\alpha(m) \mid k$. By (b) we find that in fact, $\alpha(m) = k$. Thus, $\pi(m) = k$, $2k$, or $4k$.

If $\pi(m) = 4k$, then $\omega(m) = 4$ and by Theorem 3.1, $\alpha(m)$ must be odd. However, $\alpha(m) \equiv 2 \pmod 4$, so this can't be the case.

If $\pi(m) = 2k$, then $\pi(m) \equiv 4 \pmod 8$, and so Theorem 2.1(2)($\Rightarrow$) implies $m \nmid L_{\pi(m)/4}$; that is, $m \nmid L_{k/2}$. But this contradicts our hypothesis (a) that $m \mid L_{k/2}$, and so $\pi(m) \ne 2k$.

We must conclude that $\pi(m) = k$ and the proof is complete. $\square$

Proof of Theorem 2.1(2). ($\Rightarrow$) Assume $k \equiv 4 \pmod 8$ and $\pi(m) = k$. Since $\pi(m) \equiv 4 \pmod 8$, by Theorem 3.1 we know that $\omega(m) = 2$ or 4. In either case, $m \mid F_{k/2}$ and $m \nmid F_q$ where $q \mid \frac{k}{2}$ and $q \neq \frac{k}{2}, \frac{k}{4}$. Thus, it only remains to prove that $m \nmid L_{k/4}$.

For ease of notation, let $s = F_{k/2+1}$, let $a = F_{k/4+1}$, and observe that $s \not\equiv 1 \pmod m$.

Claim 1. $F_{k/4-1} \equiv -sa \pmod m$.

Proof of Claim 1. Modulo m, the Fibonacci sequence starting at $F_{k/2}$ is $0, s, s, 2s, 3s, 5s, \ldots$, and in general, $F_{k/2+n} \equiv sF_n \pmod m$. In particular, $F_{(3k)/4+1} \equiv sa$. The identity $F_{-n} = (-1)^{n+1}F_n$ implies $F_{k-n} \equiv F_{-n} \equiv (-1)^{n+1}F_n \pmod m$. Since $\frac{k}{4}$ is odd, we find,

$$F_{k/4-1} \equiv F_{k-((3k)/4+1)} \equiv -F_{(3k)/4+1} \equiv -sa \pmod m.$$

Claim 2. $(a, m) = 1$.

Proof of Claim 2. We have $(F_{k/4-1}, F_{k/4+1}) = F_{(k/4-1,k/4+1)} = F_2 = 1$. So, there exist integers u and v such that $F_{k/4-1}u + F_{k/4+1}v = 1$. Thus, $-sau + av \equiv 1 \pmod m$, and so $a(-su + v) \equiv 1 \pmod m$ and we find that a is invertible mod m. That is, $(a, m) = 1$.

Consider the identity $L_n = F_{n-1} + F_{n+1}$. For contradiction,

$$\begin{aligned} m \mid L_{k/4} \implies m \mid F_{k/4-1} + F_{k/4+1} &\implies -sa + a \equiv 0 \pmod m \\ \implies a(1-s) \equiv 0 \pmod m &\implies s \equiv 1 \pmod m. \end{aligned}$$

The last implication is due to the fact that $(a, m) = 1$, and we've arrived at a contradiction since $s \not\equiv 1 \pmod m$. We conclude $m \nmid L_{k/4}$, as needed.

($\Leftarrow$) Assume $k \equiv 4 \pmod 8$, (a) $m \mid F_{k/2}$, (b) $m \nmid L_{k/4}$, and (c) $m \nmid F_q$ for all $q \mid k$ where $q \neq \frac{k}{2}$ or $\frac{k}{4}$. We must prove that $\pi(m) = k$. By (a) and (c), $\alpha(m) = \frac{k}{4}$ or $\frac{k}{2}$. We know that the only possible values for $\omega(m)$ are 1, 2, or 4.

Case 1: $\alpha(m) = \frac{k}{4}$.

If $\omega(m) = 2$, then $\pi(m) = \frac{k}{2} \equiv 2 \pmod 4$. However this contradicts Theorem 3.1 since $\pi(m) \equiv 2 \pmod 4$ if and only if $\omega(m) = 1$.

If $\omega(m) = 1$, then $\pi(m) = \frac{k}{4} \equiv 1 \pmod 2$. Again, this contradicts Theorem 3.1 since $\omega(m) = 1$ if and only if $\pi(m) \equiv 2 \pmod 4$.

Thus, in Case 1 we find that $\omega(m) = 4$ and we conclude $\pi(m) = k$.

Case 2: $\alpha(m) = \frac{k}{2}$.

If $\omega(m) = 4$, then $\pi(m) = 2k \equiv 0 \pmod 8$. But by Theorem 3.1, if $\pi(m) \equiv 0 \pmod 8$, then $\omega(m) = 2$, a contradiction.

If $\omega(m) = 1$, then $\pi(m) = \frac{k}{2} \equiv 2 \pmod 4$. We can now apply Theorem 2.1(1)($\Rightarrow$), and we find $m \mid L_{\pi(m)/2} = L_{k/4}$. However, this contradicts our hypothesis (b).

Thus, in Case 2 we find $\omega(m) = 2$ and we conclude $\pi(m) = k$. $\square$

Proof of Theorem 2.1(3). ($\Rightarrow$) Assume $k \equiv 0 \pmod 8$ and $\pi(m) = k$. Since $\pi(m) \equiv 0 \pmod 8$, Theorem 3.1 tells us that $\omega(m) = 2$, and so $\alpha(m) = \frac{k}{2}$. Thus, $m \mid F_{k/2}$ and $m \nmid F_q$ for any q such that $1 \leq q < \frac{k}{2}$. In particular, $m \nmid F_q$ for all q such that $q \mid \frac{k}{2}$ and $q \neq \frac{k}{2}$, and this direction of the proof is complete.

($\Leftarrow$) Assume $k \equiv 0 \pmod 8$, and (a) $m \mid F_{k/2}$, and (b) $m \nmid F_q$ for all q such that $q \mid \frac{k}{2}$ and $q \neq \frac{k}{2}$. We must prove that $\pi(m) = k$. By (a), we see $\alpha(m) \mid \frac{k}{2}$, and by (b), we deduce that in fact $\alpha(m) = \frac{k}{2}$. Thus $\alpha(m) \equiv 0 \pmod 4$. By Theorem 3.1, this can only happen when $\omega(m) = 2$. Thus $\pi(m) = k$. □

References

[Flanagan et al. 2015] P. Flanagan, M. S. Renault, and J. Updike, "Symmetries of Fibonacci points, mod m", *Fibonacci Quart.* **53**:1 (2015), 34–41. MR

[Gupta et al. 2012] S. Gupta, P. Rockstroh, and F. E. Su, "Splitting fields and periods of Fibonacci sequences modulo primes", *Math. Mag.* **85**:2 (2012), 130–135. MR Zbl

[Renault 1996] M. Renault, *The Fibonacci sequence under various moduli*, master's thesis, Wake Forest University, 1996, available at http://webspace.ship.edu/msrenault/fibonacci/FibThesis.pdf.

[Robinson 1963] D. W. Robinson, "The Fibonacci matrix modulo m", *Fibonacci Quart* **1**:2 (1963), 29–36. MR Zbl

[Stein et al. 2016] W. A. Stein et al., *Sage mathematics software*, Version 6.7, Sage Development Team, 2016, available at http://www.sagemath.org.

[Vinson 1963] J. Vinson, "The relation of the period modulo to the rank of apparition of m in the Fibonacci sequence", *Fibonacci Quart* **1**:2 (1963), 37–45. MR Zbl

[Wall 1960] D. D. Wall, "Fibonacci series modulo m", *Amer. Math. Monthly* **67** (1960), 525–532. MR Zbl

Received: 2016-06-02 Accepted: 2017-09-09

ajdish@udel.edu
Department of Mathematical Sciences, University of Delaware, Newark, DE, United States

msrenault@ship.edu
Mathematics Department, Shippensburg University, Shippensburg, PA, United States

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2018 is US $190/year for the electronic version, and $250/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2018 vol. 11 no. 5