The Period, Rank, and Order of the (a, b)-Fibonacci Sequence Mod m

MARC RENAULT
Shippensburg University
Shippensburg, PA 17257
msrenault@ship.edu

The Fibonacci sequence $F = 0, 1, 1, 2, 3, 5, 8, \ldots$ has intrigued mathematicians for centuries, as it seems there is no end to its many surprising properties. Of particular interest to us are its properties when reduced under a modulus. It is well known, for example, that $F \pmod m$ is periodic, that the zeros are equally spaced, and that each period of $F \pmod m$ contains exactly 1, 2, or 4 zeros. We'll denote the period of $F \pmod m$ by $\pi(m)$. Formulas are known for computing $\pi(m)$ based on the prime factorization of m, but if p is prime, there is no formula for $\pi(p)$. However, certain divisibility relations hold: $\pi(p) \mid p - 1$ if $p \equiv \pm 1 \pmod{10}$, and $\pi(p) \mid 2(p + 1)$ if $p \equiv \pm 3 \pmod{10}$.

This paper arose from the realization that many of the modulo m properties of the Fibonacci sequence are also properties of a much larger class of sequences. Further, matrix methods offer elementary proofs for the general case that are no more difficult than for the Fibonacci sequence itself.

For integers a and b, we define the (a, b)-*Fibonacci sequence* F as the sequence with initial conditions $F_0 = 0$, $F_1 = 1$, that satisfies the general second-order linear recurrence relation $F_n = aF_{n-1} + bF_{n-2}$. So, for example, the $(1, 1)$-Fibonacci sequence is the classic case $F = 0, 1, 1, 2, 3, 5, \ldots$, and the $(3, -2)$-Fibonacci sequence begins $0, 1, 3, 7, 15, 31, \ldots$. In general, $F = 0, 1, a, a^2 + b, a^3 + 2ab, \ldots$. In this article, we examine the behavior of the (a, b)-Fibonacci sequence under a modulus.

When reducing the (a, b)-Fibonacci sequence modulo m, we'll assume m is chosen so that $\gcd(b, m) = 1$. That way, the sequence is uniquely determined backward as well as forward. For instance, we can compute $F_{-1} \equiv b^{-1} \pmod m$. Modulo m, any pair of residues completely determines the sequence F, and there are finitely many pairs of residues, so F is periodic. We denote the period of $F \pmod m$ by $\pi(m)$.

The *rank of apparition,* or simply *rank,* of $F \pmod m$ is the least positive r such that $F_r \equiv 0 \pmod m$, and we denote the rank of $F \pmod m$ by $\alpha(m)$. If $F_{\alpha(m)+1} \equiv s \pmod m$, observe that the terms of F starting with index $\alpha(m)$, namely $0, s, as, (a^2 + b)s, \ldots$, are exactly the initial terms of F multiplied by a factor of s.

Finally, we consider the *order* of $F \pmod m$, denoted by $\omega(m)$, and defined $\omega(m) = \pi(m)/\alpha(m)$. We shall see soon that $\omega(m)$ is always an integer, and that $\omega(m) = \mathrm{ord}_m(F_{\alpha(m)+1})$, the multiplicative order of $F_{\alpha(m)+1}$ modulo m. Other authors have not named this function, but its close connection with the multiplicative order of $F_{\alpha(m)+1}$ makes the name "order" seem reasonable.

Lucas studied the (a, b)-Fibonacci sequence extensively and in 1878 established foundational results on the rank [**9**, section XXV]. He assigned $\Delta = a^2 + 4b$ and deduced that if Δ is a quadratic residue (that is, a nonzero perfect square) mod p, then $\alpha(p) \mid p - 1$. Also, if Δ is a quadratic nonresidue (a residue that is not a perfect square), then $\alpha(p) \mid p + 1$. Finally, if $p \mid \Delta$, then $\alpha(p) = p$. These results were all

Math. Mag. **86** (2013) 372–380. doi:10.4169/math.mag.86.5.372.

obtained using the identity

$$2^{n-1}F_n = \binom{n}{1}a^{n-1} + \binom{n}{3}a^{n-3}\Delta + \binom{n}{5}a^{n-5}\Delta^2 + \cdots$$

Other authors followed by generalizing these results, or providing alternate proofs. See, e.g., [**1, 3, 6, 17**].

In 1960, Wall [**16**] produced results on the period of the (1, 1)-Fibonacci sequence and on the period of any integer sequence G satisfying $G_n = G_{n-1} + G_{n-2}$. Wall's paper seems to have renewed interest in the subject. In 1963, Vinson [**15**] and Robinson [**12**] both extended Wall's work; Vinson studied the order of the (1, 1)-Fibonacci sequence, and Robinson reproduced many results of Wall and Vinson, but with proofs greatly simplified by use of matrix methods. 1963 was also the year the *Fibonacci Quarterly* was established, and throughout the years many papers on the Fibonacci sequence modulo m have appeared there.

The study of generalized Fibonacci sequences under a modulus has continued in more recent years, and articles on the topic appear occasionally in this MAGAZINE. See, e.g., [**5, 8, 13, 14**]. See also [**7**] for a non-modular treatment of the (a, b)-Fibonacci sequence.

Through our study of the (a, b)-Fibonacci sequence modulo m, we hope to bring together many of the previous results, generalizing to the (a, b) case where necessary, and presenting them as a cohesive whole, using matrices as our main tool to supply elementary proofs.

Preliminaries

The matrix $A = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]$ has the wonderful property that

$$A^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix},$$

where F here is the usual (1, 1)-Fibonacci sequence. This fact is extremely useful for the computation of very large Fibonacci numbers, and for finding and proving properties of F. Many authors use the matrix $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right]$, but in this article we will follow the notation found in [**12**] and [**7**]; see [**4**] for more on the use of this and other matrices.

Let F denote the general (a, b)-Fibonacci sequence, let U denote the (a, b)-Fibonacci matrix below, and observe the form of U^n, which is easily confirmed by induction:

$$U = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}, \qquad U^n = \begin{bmatrix} bF_{n-1} & F_n \\ bF_n & F_{n+1} \end{bmatrix}.$$

Consequently, $U^{\pi(m)} \equiv I \pmod{m}$. Moreover, if $F_n \equiv 0$, then $F_{n-1} \equiv b^{-1}F_{n+1}$; thus, $U^{\alpha(m)} \equiv sI \pmod{m}$ for some integer s.

Observe that $\det U = -b$. Thus, $(-b)^{\pi(m)} = (\det U)^{\pi(m)} = \det U^{\pi(m)} \equiv 1 \pmod{m}$. So,

$$\operatorname{ord}_m(-b) \mid \pi(m).$$

This proves the well-known result for the (1, 1)-Fibonacci sequence that $\pi(m)$ is even for any $m > 2$.

The exponents n for which $U^n \equiv I \pmod{m}$ form a simple arithmetic progression ($U^0 \equiv I$, and if $U^i \equiv U^j \equiv I$, then $U^{i+j} \equiv I$). Thus,

$$U^n \equiv I \iff \pi(m) \mid n.$$

Similarly, the exponents n for which U^n is congruent to a scalar multiple of I form a simple arithmetic progression, and so

$$U^n \equiv sI \quad \text{for some} \quad s \in \mathbb{Z} \iff \alpha(m) \mid n.$$

From this we see that $\alpha(m) \mid \pi(m)$.

We defined the order of $F \pmod{m}$ as $\omega(m) = \pi(m)/\alpha(m)$, but $\omega(m)$ has another interpretation. If $U^{\alpha(m)} \equiv sI$, then $\operatorname{ord}_m(s)$ is the least positive value of k such that $U^{k\alpha(m)} \equiv I$. Consequently, $\operatorname{ord}_m(s)$ is the least positive k such that $\pi(m) \mid k\alpha(m)$. Clearly, the smallest such k is $\omega(m)$. Thus,

$$\text{If } U^{\alpha(m)} \equiv sI, \text{ then } \omega(m) = \operatorname{ord}_m(s).$$

Computing $\pi(m)$ and $\alpha(m)$

Much of our work in this paper is conducted with an eye toward constructing an algorithm that, given a, b, and m, will produce the period and rank of the (a, b)-Fibonacci sequence modulo m. The first step is recognizing that it is easy to compute $\pi(m)$ once we know $\pi(p^e)$ for all prime power factors p^e of m. The same idea holds for computing $\alpha(m)$.

The following theorem gives us the tool we need, and it is well known for the (1, 1)-Fibonacci sequence; see, e.g., [**15**]. In fact, our statement of the theorem for the (a, b) case is exactly the same as that for the (1, 1) case.

THEOREM 1. *Let brackets denote the least common multiple operation.*

(a) $\alpha([m_1, m_2]) = [\alpha(m_1), \alpha(m_2)]$

(b) $\pi([m_1, m_2]) = [\pi(m_1), \pi(m_2)]$

Proof. Let $m = [m_1, m_2]$.

Part (a). Let $\alpha = \alpha(m)$, $\alpha_1 = \alpha(m_1)$, and $\alpha_2 = \alpha(m_2)$. Since $F_\alpha \equiv 0 \pmod{m}$, we have $F_\alpha \equiv 0 \pmod{m_i}$ for each $i = 1, 2$. Thus, $\alpha_i \mid \alpha$ for each $i = 1, 2$ and we get $[\alpha_1, \alpha_2] \mid \alpha$.

Conversely, we know $F_{[\alpha_1,\alpha_2]} \equiv 0 \pmod{m_i}$ for each $i = 1, 2$, so $F_{[\alpha_1,\alpha_2]} \equiv 0 \pmod{m}$. Thus, $\alpha \mid [\alpha_1, \alpha_2]$.

Part (b). Let $\pi = \pi(m)$, $\pi_1 = \pi(m_1)$, and $\pi_2 = \pi(m_2)$. Since $U^\pi \equiv I \pmod{m}$, we have $U^\pi \equiv I \pmod{m_i}$ for each $i = 1, 2$. Thus, $\pi_i \mid \pi$ for each $i = 1, 2$ and we get $[\pi_1, \pi_2] \mid \pi$.

Conversely, we know $U^{[\pi_1,\pi_2]} - I \equiv 0 \pmod{m_i}$ for each $i = 1, 2$, and it follows that $U^{[\pi_1,\pi_2]} - I \equiv 0 \pmod{m}$. Thus, $\pi \mid [\pi_1, \pi_2]$. ∎

COROLLARY. *If $m_1 \mid m_2$, then $\alpha(m_1) \mid \alpha(m_2)$ and $\pi(m_1) \mid \pi(m_2)$.*

To apply the above theorem, suppose that $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then $\alpha(m) = \left[\alpha(p_1^{e_1}), \alpha(p_2^{e_2}), \ldots, \alpha(p_k^{e_k})\right]$ and $\pi(m) = \left[\pi(p_1^{e_1}), \pi(p_2^{e_2}), \ldots, \pi(p_k^{e_k})\right]$.

Much more generally, Theorem 1 and its proof work for recurrence relations of any order, $S_n = a_1 S_{n-1} + a_2 S_{n-2} + \cdots + a_k S_{n-k}$. The theorem can even be used (with slight modification) when the modulus is not relatively prime to a_k (in which case the sequence cannot be uniquely determined for negative subscripts). See [**2**, p. 220] for a very general statement and interpretation of the theorem.

We now turn our attention to computing $\alpha(p^e)$ and $\pi(p^e)$, where p is a prime and e is a positive integer.

Computing $\pi(p^e)$ and $\alpha(p^e)$

It turns out that we can express $\pi(p^e)$ and $\alpha(p^e)$ in terms of $\pi(p)$ and $\alpha(p)$. The main result of this section, Theorem 2, shows exactly how to do that.

The proofs in this section follow those of [**12**], generalized to the (a, b) case. Again, the results here for general a and b are almost exactly those one finds in the literature for the (1, 1)-Fibonacci sequence; the slight differences are noted at the end of the section.

We begin by seeing how $\alpha(p^e)$ and $\alpha(p^{e+1})$ are related, and likewise for π.

PROPOSITION 1. *For any prime p and for any integer $e \geq 1$, $\alpha(p^{e+1}) = \alpha(p^e)$ or $p \cdot \alpha(p^e)$. Similarly, $\pi(p^{e+1}) = \pi(p^e)$ or $p \cdot \pi(p^e)$.*

Proof. Suppose that $U^n \equiv sI \pmod{p^e}$ for some integer s. Then $U^n = sI + p^e B$ for some matrix B. Then $U^{pn} = (sI + p^e B)^p = s^p I + \binom{p}{1} s^{p-1} p^e B + \cdots$, where every term after the first is divisible by p^{e+1}. Thus, $U^{pn} \equiv s^p I \pmod{p^{e+1}}$.

Now if $n = \alpha(p^e)$, then the conditions in the first line of this proof are satisfied, and we conclude that $\alpha(p^{e+1}) \mid p\alpha(p^e)$. But of course $\alpha(p^e) \mid \alpha(p^{e+1})$, and we conclude that $\alpha(p^{e+1}) = \alpha(p^e)$ or $p\alpha(p^e)$.

Similarly, if $n = \pi(p^e)$, then again the above conditions are satisfied (with $s = 1$) and we find that $\pi(p^{e+1}) = \pi(p^e)$ or $p\pi(p^e)$. ∎

Thus, for each unit increase in e, $\alpha(p^e)$ either stays the same or increases by a factor of p. In fact, the next result shows that there is more going on: $\alpha(p^e)$ may stay constant initially, but once it starts to increase, it *must* continue increasing. The same is true of $\pi(p^e)$.

PROPOSITION 2. *Except for the single case $p = 2$ and $e = 1$, the following holds for any prime p and positive integer e.*

(a) *If $\alpha(p^e) \neq \alpha(p^{e+1})$, then $\alpha(p^{e+1}) \neq \alpha(p^{e+2})$.*
(b) *If $\pi(p^e) \neq \pi(p^{e+1})$, then $\pi(p^{e+1}) \neq \pi(p^{e+2})$.*

Proof. Suppose that $U^n \equiv sI \pmod{p^e}$ and that U^n is not congruent to any scalar multiple of $I \pmod{p^{e+1}}$. Then $U^n = sI + p^e B$, where $p^e B$ is not congruent to any scalar multiple of $I \pmod{p^{e+1}}$. Consequently, B is not congruent to any scalar multiple of $I \pmod{p}$.

Now $U^{pn} = (sI + p^e B)^p = s^p I + \binom{p}{1} s^{p-1} p^e B + \cdots$, and all terms replaced by the ellipsis are divisible by p^{e+2}. (This last statement is where we require any case other than $p = 2$ and $e = 1$.)

So, $U^{pn} \equiv s^p I \pmod{p^{e+1}}$. Moreover, since $p^{e+1} B$ is not congruent to any scalar multiple of $I \pmod{p^{e+2}}$, we also know that U^{pn} is not congruent to any scalar multiple of $I \pmod{p^{e+2}}$.

If $n = \alpha(p^e)$ and $\alpha(p^e) \neq \alpha(p^{e+1})$, then by Proposition 1, $pn = \alpha(p^{e+1})$ and the above argument implies $\alpha(p^{e+1}) \neq \alpha(p^{e+2})$.

Similarly, if $n = \pi(p^e)$ and $\pi(p^e) \neq \pi(p^{e+1})$, then $pn = \pi(p^{e+1})$ and the above argument implies $\pi(p^{e+1}) \neq \pi(p^{e+2})$. ∎

The main result of this section is an immediate consequence and reformulation of the two preceding propositions. The last point of this theorem is deduced by inspection: modulo 2, we must have $b \equiv 1$, and so $F = 0, 1, 0, 1, \ldots$ (when $a \equiv 0$) or $F = 0, 1, 1, 0, 1, 1, \ldots$ (when $a \equiv 1$).

THEOREM 2. *Let an integer $e \geq 1$ be given.*

- *For odd p,*
  $\alpha(p^e) = p^{e-e'}\alpha(p)$, where $1 \leq e' \leq e$ is maximal so that $\alpha(p^{e'}) = \alpha(p)$.
  $\pi(p^e) = p^{e-e'}\pi(p)$, where $1 \leq e' \leq e$ is maximal so that $\pi(p^{e'}) = \pi(p)$.
- *For $p = 2$ and $e \geq 2$,*
  $\alpha(2^e) = 2^{e-e'}\alpha(4)$, where $2 \leq e' \leq e$ is maximal so that $\alpha(2^{e'}) = \alpha(4)$.
  $\pi(2^e) = 2^{e-e'}\pi(4)$, where $2 \leq e' \leq e$ is maximal so that $\pi(2^{e'}) = \pi(4)$.
- *Finally,*
  if a is odd, then $\alpha(2) = \pi(2) = 3$; if a is even, then $\alpha(2) = \pi(2) = 2$.

In the (1, 1)-Fibonacci sequence, it is an open problem whether any primes p exist such that $\pi(p^2) = \pi(p)$. Despite extensive searching, none have been found [**10**]. Even if such a p is found, there must exist *some* maximal e' such that $\pi(p^{e'}) = \pi(p)$, since no (1, 1)-Fibonacci number (other than F_0) is divisible by infinitely many powers of p.

However, in the more general (a, b) setting, we can find examples where $\pi(p^2) = \pi(p)$. Fix $a = 76$ and $b = 56$, and consider the behavior of $F \pmod{3^e}$ as e increases:

m	3	3^2	3^3	3^4	3^5	3^6	3^7	3^8
$\pi(m)$	6	6	18	54	162	486	1458	4374
$\alpha(m)$	3	3	3	3	3	3	9	27

We conclude that $\pi(3^e) = 3^{e-2} \cdot 6$ for $e \geq 2$, and $\alpha(3^e) = 3^{e-6} \cdot 3$ for $e \geq 6$.

We can also find examples where $\alpha(p^e)$ or $\pi(p^e)$ is constant for all e. If $a = 2$ and $b = -4$, then $F = 0, 1, 2, 0, -8, \ldots$. Consequently, for any odd prime p, $\alpha(p^e) = 3$ for all e and $\pi(p^e) = 3 \cdot \mathrm{ord}_{p^e}(-8)$. Finally, we might consider the case $a = 1$ and $b = -1$. In this situation, $F = 0, 1, 1, 0, -1, -1, 0, 1 \ldots$. Thus, for any odd prime p, $\alpha(p^e) = 3$ and $\pi(p^e) = 6$ for all positive integers e.

Computing $\pi(p)$ and $\alpha(p)$

Unfortunately, there are no explicit formulas for evaluating $\pi(p)$ and $\alpha(p)$. Perhaps this is not surprising, since $\pi(p)$ is the order of a matrix modulo p, and there is no explicit formula for computing the order of an integer modulo p. However, we do have divisibility relations.

By Theorem 2, we have $\alpha(2) = \pi(2) = 3$ or $\alpha(2) = \pi(2) = 2$. For the remainder of this section, we will assume that p is an odd prime.

The matrix U has characteristic polynomial $c(x) = x^2 - ax - b$. This polynomial has a root modulo p if the discriminant $a^2 + 4b$ is a perfect square modulo p. Specifically, if δ is an integer with the property that $\delta^2 \equiv a^2 + 4b \pmod{p}$, then the roots of $c(x) \pmod{p}$, as given by the quadratic formula, are $2^{-1}(a \pm \delta)$. The following theorem shows that we can gain insight into the divisibility properties of $\alpha(p)$ and $\pi(p)$ by considering the nature of $a^2 + 4b$.

THEOREM 3. *Let $\Delta = a^2 + 4b$ and let p be an odd prime such that $p \nmid b$. Then modulo p,*

(a) *if Δ is a (nonzero) quadratic residue, then $\alpha(p) \mid p - 1$ and $\pi(p) \mid p - 1$.*
(b) *if Δ is a quadratic nonresidue, then $\alpha(p) \mid p + 1$ and $\pi(p) \mid (p + 1)\mathrm{ord}_p(-b)$; also, except in the case $b \equiv -1$, $\pi(p) \nmid p + 1$.*
(c) *if $\Delta \equiv 0$, then $\alpha(p) = p$ and $\pi(p) = p \cdot \mathrm{ord}_p(2^{-1}a)$.*

Proof. For parts (a) and (b), we sketch the proofs found in [**5**].

(a) Suppose that Δ is a quadratic residue, modulo p. Then the characteristic polynomial $c(x)$ of U has two distinct roots, call them λ_1 and λ_2. Thus, U is diagonalizable and can be written $U \equiv PDP^{-1}$, where P is the matrix with eigenvectors as columns and

$$D \equiv \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

Applying Fermat's Little Theorem, we find $D^{p-1} \equiv I$. Thus, $U^{p-1} \equiv I$ and part (a) of the theorem follows.

(b) Suppose that Δ is a quadratic nonresidue, modulo p. In this case, we switch our view from working with integers and congruences to working within the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The polynomial $c(x)$ is irreducible in $\mathbb{F}_p$, but we can create a field extension $\mathbb{F}_p[\gamma]$ where γ has the property that $c(\gamma) = 0$. It is shown easily in [**5**] that $\gamma^p \neq \gamma$ and $c(\gamma^p) = 0$; thus $c(x)$ has two distinct roots in $\mathbb{F}_p[\gamma]$. So U is diagonalizable in $\mathbb{F}_p[\gamma]$ and can be written $U = PDP^{-1}$ for some matrix P and

$$D = \begin{bmatrix} \gamma & 0 \\ 0 & \gamma^p \end{bmatrix}.$$

Since $(x-\gamma)(x-\gamma^p) = x^2 - ax - b$, we have $\gamma^{p+1} = -b$. Moreover, we observe that $(\gamma^p)^{p+1} = (-b)^p = -b$, with the final equality due to Fermat's Little Theorem. Thus, $U^{p+1} = PD^{p+1}P^{-1} = P\left[\begin{smallmatrix} -b & 0 \\ 0 & -b \end{smallmatrix}\right]P^{-1} = \left[\begin{smallmatrix} -b & 0 \\ 0 & -b \end{smallmatrix}\right]$. As a result, $\alpha(p) \mid p+1$, and unless $b \equiv -1 \pmod{p}$, $\pi(p) \nmid p+1$. It also follows that $U^{(p+1)\mathrm{ord}_p(-b)} = I$ and so $\pi(p) \mid (p+1)\mathrm{ord}_p(-b)$.

(c) Suppose that $\Delta \equiv 0 \pmod{p}$. Then $c(x)$ has a repeated root, $2^{-1}a$ (and $a \not\equiv 0$, otherwise $p \mid b$, a contradiction). In this case, U is not diagonalizable, but we can put U into Jordan form: $U = PJP^{-1}$ for some invertible P. Below, we see the form of J and of J^n.

$$J \equiv \begin{bmatrix} 2^{-1}a & 1 \\ 0 & 2^{-1}a \end{bmatrix}, \qquad J^n \equiv \begin{bmatrix} (2^{-1}a)^n & n(2^{-1}a)^{n-1} \\ 0 & (2^{-1}a)^n \end{bmatrix}.$$

Since $U^n \equiv PJ^nP^{-1}$, and since scalar multiples of I commute with any matrix, we find $U^n \equiv sI$ for some integer s if and only if $J^n \equiv sI$. So, considering J^n above, $\alpha(p)$ is the least integer n such that $n(2^{-1}a)^{n-1} \equiv 0 \pmod{p}$. Since $a \not\equiv 0 \pmod{p}$, we conclude that $\alpha(p) = p$.

Working modulo p, we obtain the following.

$$\begin{aligned} U^n \equiv I &\iff J^n \equiv I \\ &\iff (2^{-1}a)^n \equiv 1 \text{ and } n(2^{-1}a)^{n-1} \equiv 0 \\ &\iff \mathrm{ord}_p(2^{-1}a) \mid n \text{ and } p \mid n \\ &\iff \mathrm{lcm}[\mathrm{ord}_p(2^{-1}a),\, p] \mid n \\ &\iff p \cdot \mathrm{ord}_p(2^{-1}a) \mid n. \end{aligned}$$

By the above, $\pi(p) = p \cdot \mathrm{ord}_p(2^{-1}a)$. ∎

The proof of part (a) also shows that if λ_1 and λ_2 are the roots of $x^2 - ax - b$, then $\pi(m) = \mathrm{lcm}[\mathrm{ord}_p(\lambda_1), \mathrm{ord}_p(\lambda_2)]$.

We've not seen the part (c) result that $\pi(p) = p \cdot \mathrm{ord}_p(2^{-1}a)$ in the literature. However, the fact that $\alpha(p) = p$ is deduced by Lucas [**9**]. Our proof for (c) appears to be

novel. It is curious that when $p \mid \Delta$, we have an explicit equality statement for $\pi(p)$ (albeit in terms of $\text{ord}_p(2^{-1}a)$, which must be calculated).

For the standard $a = 1, b = 1$ situation, $\Delta = 5$. Using the law of quadratic reciprocity, we can find that 5 is a quadratic residue when $p \equiv \pm 1 \pmod{10}$ and 5 is a quadratic nonresidue when $p \equiv \pm 3 \pmod{10}$.

Finally, we note that combining Theorem 3 with the fact that $\text{ord}_p(-b) \mid \pi(p)$ significantly narrows the possible values of $\pi(p)$, and can aid with a computer search for $\pi(p)$.

Properties of $\omega(m)$

The previous theorem showed how $\pi(p)$ and $\alpha(p)$ are related to the modulus, p. In this final section, we consider the relationship between $\alpha(m)$ and $\pi(m)$, as expressed by the function $\omega(m) = \pi(m)/\alpha(m)$. One of the most surprising things about the (1, 1)-Fibonacci sequence modulo m is that $\omega(m) = 1$, 2, or 4, no matter the value of m or the size of $\pi(m)$. Generally, however, for a fixed a and b, Theorem 4(a) shows us that $\omega(m)$ can take on infinitely many values as m varies. The following theorem and proof generalize those found in [**12**].

THEOREM 4.

(a) $\omega(m) \mid 2 \cdot \text{ord}_m(-b)$

(b) $\pi(m) = (1 \text{ or } 2) \cdot \text{lcm}[\alpha(m), \text{ord}_m(-b)]$

Proof. Suppose $U^{\alpha(m)} \equiv \left[\begin{smallmatrix} s & 0 \\ 0 & s \end{smallmatrix}\right]$. Comparing determinants, we get $s^2 \equiv (-b)^{\alpha(m)}$. Raising both sides to $\text{ord}_m(-b)$ yields $s^{2 \cdot \text{ord}_m(-b)} \equiv 1$. Since $\text{ord}_s(m) = \omega(m)$, part (a) follows.

For part (b), we note that s^2 and $(-b)^{\alpha(m)}$, being congruent modulo m, have the same multiplicative order modulo m, namely,

$$\frac{\text{ord}_m(s)}{\gcd(2, \text{ord}_m(s))} = \frac{\text{ord}_m(-b)}{\gcd(\alpha(m), \text{ord}_m(-b))}.$$

Substituting $\omega(m)$ for $\text{ord}_m(s)$ and cross-multiplying yields

$$\omega(m) \cdot \gcd(\alpha(m), \text{ord}_m(-b)) = \gcd(2, \omega(m)) \cdot \text{ord}_m(-b).$$

As a consequence,

$$\omega(m) = (1 \text{ or } 2)\frac{\text{ord}_m(-b)}{\gcd(\alpha(m), \text{ord}_m(-b))}.$$

Multiplying both sides of the equation by $\alpha(m)$ produces part (b) of the theorem.

$$\pi(m) = \omega(m)\alpha(m) = (1 \text{ or } 2) \cdot \text{lcm}[\alpha(m), \text{ord}_m(-b)]. \qquad \blacksquare$$

Theorem 4(a) gives us the interesting result that if $b = -1$, then $\omega(m)$ is always 1 or 2. We saw in the Preliminaries section that $\alpha(m) \mid \pi(m)$ and $\text{ord}_m(-b) \mid \pi(m)$, so it immediately follows that $\text{lcm}[\alpha(m), \text{ord}_m(-b)] \mid \pi(m)$; part (b) of the above theorem makes this divisibility relation much more precise. Finally, we note that part (b) provides a very quick computation of $\pi(m)$, if $\alpha(m)$ and $\text{ord}_m(-b)$ are known.

In the $a = 1, b = 1$ case, $\omega(p^e) = \omega(p)$ for any odd prime p [**11**, p. 38]. That is, π and α move in "lock step" with each other: $\pi(p^e) = \pi(p^{e+1}) \iff \alpha(p^e) = \alpha(p^{e+1})$. Our final theorem shows something similar for the general a, b setting. In the general setting, however, we find $\pi(p^e) = \pi(p^{e+1}) \implies \alpha(p^e) = \alpha(p^{e+1})$ but the converse does not hold. Almost always, as e grows, $\omega(p^e)$ eventually becomes constant.

THEOREM 5.

(a) *Let p be an odd prime. If there exists an e such that $\alpha(p^e) = \alpha(p)$, but $\alpha(p^{e+1}) \neq \alpha(p)$, then $\omega(p^{e+i}) = \omega(p^e)$ for all $i \geq 0$.*

(b) *If there exists an e such that $\alpha(2^e) = \alpha(4)$, but $\alpha(2^{e+1}) \neq \alpha(4)$, then $\omega(2^{e+1+i}) = \omega(2^{e+1})$ for all $i \geq 0$.*

Proof. (a) Given $\alpha(p^e) = \alpha(p)$ and $\alpha(p^{e+1}) \neq \alpha(p)$, we apply Proposition 1 and Proposition 2(a) to conclude that $\alpha(p^{e+1}) = p\alpha(p)$. Assume for contradiction that $\pi(p^{e+1}) = \pi(p^e)$. Then, applying Proposition 2(b), we find that $\pi(2^{e+1}) = \pi(p)$. Thus,

$$\omega(p^{e+1}) = \frac{\pi(p^{e+1})}{\alpha(p^{e+1})} = \frac{\pi(p)}{p\alpha(p)} = \frac{\omega(p)}{p}.$$

Therefore, $p \mid \omega(p)$. But by Theorem 4(a), $\omega(p) \mid 2 \cdot \mathrm{ord}_p(-b)$. Since p is odd, $p \mid \mathrm{ord}_p(-b)$. But this is clearly a contradiction since $\mathrm{ord}_p(-b) \mid p - 1$.

Thus, our assumption was wrong, $\pi(p^{e+1}) \neq \pi(p^e)$, and so $\omega(p^e) = \omega(p^{e+1}) = \omega(p^{e+2}) = \cdots$.

The proof for part (b) is similar. Given $\alpha(2^e) = \alpha(4)$ and $\alpha(2^{e+1}) \neq \alpha(4)$, we conclude that $\alpha(2^{e+2}) = 4\alpha(4)$. Assume for contradiction that $\pi(2^{e+2}) = \pi(2^{e+1})$; then $\pi(2^{e+2}) = \pi(4)$. Thus,

$$\omega(2^{e+2}) = \frac{\pi(2^{e+2})}{\alpha(2^{e+2})} = \frac{\pi(4)}{4\alpha(4)} = \frac{\omega(4)}{4} = \frac{1 \text{ or } 2}{4}.$$

The last equality above is due to inspection: Since $\omega(2) = 1$, $\omega(4) = 1$ or 2. But $\omega(2^{e+2})$ must be an integer, so a contradiction has been found.

Thus, $\pi(2^{e+2}) \neq \pi(2^{e+1})$, and so $\omega(2^{e+1}) = \omega(2^{e+2}) = \omega(2^{e+3}) = \cdots$. ∎

The hypothesis in Theorem 5, that $\alpha(p^e) \neq \alpha(p)$ for some e, is almost always satisfied. In fact, if $\alpha(p^e) = \alpha(p)$ for all e, then we must have $F_{\alpha(p)} = 0$ (*equality*, not just congruence), a very strong requirement indeed. We previously noted the case $a = 2, b = -4$ in which $\alpha(p^e) = 3$ for all positive e, but $\pi(p^e)$ grows as e increases. In this case, $\omega(p^e)$ increases without bound.

For the (1, 1)-Fibonacci sequence, we noted that p odd implies $\omega(p^e)$ is constant as e grows. In the general a and b situation, more interesting behavior can be observed. Consider again the example $a = 76$ and $b = 56$, and observe the behavior of $F \pmod{3^e}$ as e increases:

m	3	3^2	3^3	3^4	3^5	3^6	3^7	3^8
$\pi(m)$	6	6	18	54	162	486	1458	4374
$\alpha(m)$	3	3	3	3	3	3	9	27
$\omega(m)$	2	2	6	18	54	162	162	162

In the above table, we see that $\omega(3^e)$ is initially constant, and then grows for a few terms before eventually stabilizing at 162.

We admit that the behavior of $\omega(p^e)$, when generalized from the (1, 1) case to the general (a, b) case, loses some of its simple elegance. On the other hand, we are reminded once again of the many fascinating properties these sequences hold, and our imagination is stirred to try to understand them even better.

Acknowledgment I would like to extend my sincere appreciation to Josh Ide who, as an undergraduate student several years ago, spent many hours in my office discussing the Fibonacci sequence and modular arithmetic. As

a teacher, I hope to motivate students and ignite their curiosity about mathematics. However, it was Josh, through his insight and dedication, who inspired me to dig deeper into this topic.

REFERENCES

1. R. D. Carmichael, On sequences of integers defined by recurrence relations, *Quart. J. Math.* **41** (1920) 343–372.
2. Paul Cull, Mary Flahive, and Robby Robson, *Difference Equations,* Springer, New York, 2005.
3. H. T. Engstrom, On sequences defined by linear recurrence relations, *Trans. Amer. Math. Soc.* **33** (1931) 210–218. http://dx.doi.org/10.1090/S0002-9947-1931-1501585-5
4. H. W. Gould, A history of the Fibonacci Q-matrix and a higher-dimensional problem, *Fib. Quart.* **19**(3) (1981) 250–257.
5. Sanjai Gupta, Parousia Rockstroh, and Francis Edward Su, Splitting fields and periods of Fibonacci sequences modulo primes, *Math. Mag.* **85** (2012) 130–135. http://dx.doi.org/10.4169/math.mag.85.2.130
6. Marshall Hall, Divisors of second-order sequences, *Bull. Amer. Math. Soc.* **43** (1937) 78–80. http://dx.doi.org/10.1090/S0002-9904-1937-06497-4
7. Dan Kalman and Robert Mena, The Fibonacci numbers—exposed, *Math. Mag.* **76** (2003) 167–181. http://dx.doi.org/10.2307/3219318
8. Hua-Chieh Li, On second-order linear recurrence sequences: Wall and Wyler revisited, *Fib. Quart.* **37** (1999) 342–349.
9. Lucas, Eduoard, Théorie des fonctions numériques simplement périodiques, *Amer. J. of Math.* **1** (1878) 184–240, 289–321. http://dx.doi.org/10.2307/2369308
10. R. J. McIntosh and E. L. Roettger, A search for Fibonacci-Wieferich and Wolstenholme primes, *Math. Comp.* **76** (2007) 2087–2094. http://dx.doi.org/10.1090/S0025-5718-07-01955-2
11. Marc Renault, *Properties of the Fibonacci Sequence Under Various Moduli,* Master's thesis, Wake Forest University, May 1996. Available at http://webspace.ship.edu/msrenault/fibonacci/FibThesis.pdf.
12. D. W. Robinson, The Fibonacci matrix modulo m, *Fib. Quart.* **1** (1963) 29–36.
13. Dominic Vella and Alfred Vella, Cycles in the generalized Fibonacci sequence modulo a prime, *Math. Mag.* **74** (2002) 294–299.
14. Dominic Vella and Alfred Vella, Calculating exact cycle lengths in the generalized Fibonacci sequence modulo p, *Math. Gaz.* **90** (2006) 70–76.
15. John Vinson, The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence, *Fib. Quart.* **1** (1963) 37–45.
16. D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960) 525–532. http://dx.doi.org/10.2307/2309169
17. Morgan Ward, Prime divisors of second-order recurring sequences, *Duke Math. J.* **21** (1954) 607–614. http://dx.doi.org/10.1215/S0012-7094-54-02163-8

Summary For given integers a and b, we consider the (a, b)-Fibonacci sequence F defined by $F_0 = 0$, $F_1 = 1$, and $F_n = aF_{n-1} + bF_{n-2}$. Given $m \geq 2$ relatively prime to b, $F \pmod m$ is periodic with period denoted $\pi(m)$. The rank of $F \pmod m$, denoted $\alpha(m)$, is the least positive r such that $F_r \equiv 0 \pmod m$, and the order of $F \pmod m$, denoted $\omega(m)$, is $\pi(m)/\alpha(m)$. In this article, we pull together results on $\pi(m)$, $\alpha(m)$, and $\omega(m)$ from the classic case $a = 1$, $b = 1$, and generalize their proofs to accommodate arbitrary integers a and b. Matrix methods are used extensively to provide elementary proofs.