ON THE DIVISIBILITY OF FIBONACCI SEQUENCES BY PRIMES OF INDEX TWO

SAM VANDERVELDE

ABSTRACT. In this paper we present several novel properties of the Wythoff array. For instance, we prove that every pair of integers occurs precisely once within the array and describe an effective means for locating any particular pair. We then observe that certain primes p, including 13, 17, 29, 37, and 41, appear to divide exactly half of all Fibonacci sequences that are regular $\bmod p$. Finally, we define the norm N of a Fibonacci sequence and demonstrate that the value of the Legendre symbol $\left(\frac{N}{p}\right)$ may be used to predict whether or not the Fibonacci sequence is divisible by p.

1. INTRODUCTION

Brother Alfred has characterized primes dividing every Fibonacci sequence [2] based on their period and congruence class $\pmod{20}$. More recently, in [4] Ballot and Elia have described the set of primes dividing the Lucas sequence, meaning they divide some term of the sequence. Our purpose here is to extend the results of the former paper utilizing the methods of the latter. In particular we will investigate primes dividing "half of all Fibonacci sequences," defined in our case via their index rather than period. We will establish a simple criterion for determining whether or not such a prime divides a given Fibonacci sequence based on whether or not the norm of that sequence is a quadratic residue modulo the prime.

The discussion is organized as follows. We begin by giving a concise development of the Wythoff array, in which we adopt a novel approach and provide new proofs of well-known properties. In the following section we define the norm of a Fibonacci sequence, so-named because this value is given by the algebraic norm of the element of the ring of integers $\mathbb{Z}[\varphi]$ used to generate that sequence. After presenting several properties of the norm we define the index of a prime p relative to the Fibonacci sequence and relate this notion to the multiplicative index of the element $-\varphi^2$ modulo a prime over p in $\mathbb{Z}[\varphi]$. We next employ these ideas to prove the criterion for when a Fibonacci sequence is divisible by a prime of index 2, then conclude with several observations and examples.

Finally, before beginning we acknowledge the many results that have already been found regarding divisibility of Fibonacci sequences by primes, as presented in [5, 6, 10, 14, 17], for instance.

2. THE WYTHOFF ARRAY REVISITED

For our purposes, a Fibonacci sequence will refer to any nonzero, doubly infinite sequence of integers in which each term is the sum of the previous two. To begin, we reimagine the Wythoff array, defined by Morrison in [13], as the natural arrangement of all Fibonacci sequences. This is accomplished via the following two observations.

Proposition 2.1. *Let $\{a_k\}_{k\in\mathbb{Z}}$ be a Fibonacci sequence and let $\varphi = \frac{1}{2}(1+\sqrt{5})$. Then we have $\frac{1}{\varphi} < a_{k+1} - a_k\varphi \leq \varphi$ for a unique $k \in \mathbb{Z}$.*

Proof. Define $\delta_k = a_{k+1} - a_k\varphi$, and note that $\delta_k \neq 0$ for any k. We find that

$$\varphi\delta_{k+1} = a_{k+2}\varphi - a_{k+1}\varphi^2 = (a_k + a_{k+1})\varphi - a_{k+1}(1+\varphi) = a_k\varphi - a_{k+1} = -\delta_k. \tag{2.1}$$

Therefore, $\delta_{k+1} = -\frac{1}{\varphi}\delta_k$. Since the values of δ_k alternate sign and decrease in magnitude by a factor of $\frac{1}{\varphi}$ for successive values of k, the claim follows. □

By reindexing if necessary, we can assume that $\delta_0 = a_1 - a_0\varphi$ falls in the given range. In what follows we will always number Fibonacci sequences in this manner. We next identify all pairs of integers satisfying this condition.

Proposition 2.2. *For $a_0, a_1 \in \mathbb{Z}$ we have $\frac{1}{\varphi} < a_1 - a_0\varphi \leq \varphi$ if and only if $a_1 = \lfloor (a_0+1)\varphi \rfloor$.*

Proof. Suppose that $\frac{1}{\varphi} < a_1 - a_0\varphi \leq \varphi$ for $a_0, a_1 \in \mathbb{Z}$. Rearranging yields

$$(a_0+1)\varphi - 1 < a_1 \leq (a_0+1)\varphi. \tag{2.2}$$

Since a_1 is an integer within this interval of unit length, we must have $a_1 = \lfloor (a_0+1)\varphi \rfloor$. These steps are clearly reversible, completing the argument. □

It follows that there exists a unique Fibonacci sequence corresponding to each $a_0 \in \mathbb{Z}$, which provides a natural means for ordering the set of all such sequences. Arranging them as an array of integers with the values of a_0 above one another yields the Wythoff array, displayed in Figure 1. The obvious candidates for the central row and column are the Fibonacci numbers and the integers, shown in boldface. The Beatty sequence for φ appears to the right of the central column.

The preceding discussion also implies that every nonzero pair of integers (m, n) appears exactly once as adjacent terms in the array, since each pair generates a Fibonacci sequence. For instance, the pairs $(1, n)$ for $-4 \leq n \leq 5$ are visible in Figure 1. In fact, it is possible to pinpoint the precise location of a given pair without much difficulty. Let us number the rows by the value of a_0 and number the columns according to their location relative to the central column. Given a pair (m, n), determine the integer t for which

$$\frac{1}{\varphi} < \frac{n - m\varphi}{(-\varphi)^t} \leq \varphi, \tag{2.3}$$

so advancing t places within the Fibonacci sequence containing (m, n) brings us to a_0. By a well-known formula $a_0 = F_{t-1}m + F_t n$, giving the row number of the sequence, while the column is just $-t$. To illustrate, let us ascertain the location of the pair $(1492, 2013)$ within the Wythoff array. One calculates

$$\frac{2013 - 1492\varphi}{(-\varphi)^{13}} \approx 0.7699, \qquad 1492F_{12} + 2013F_{13} = 683877.$$

Hence, 1492 and 2013 appear as terms -13 and -12 of row 683877.

Recall that given a Fibonacci sequence $\{a_k\}_{k\in\mathbb{Z}}$ we set $\delta_k = a_{k+1} - a_k\varphi$ and index the terms so that $\frac{1}{\varphi} < \delta_0 \leq \varphi$. The proof of Proposition 2.1 demonstrates that

$$-1 \leq \delta_1 < -\frac{1}{\varphi^2}, \quad -\frac{1}{\varphi^2} \leq \delta_3 < -\frac{1}{\varphi^4}, \quad -\frac{1}{\varphi^4} \leq \delta_5 < -\frac{1}{\varphi^6}, \ \ldots,$$
$$\frac{1}{\varphi^3} < \delta_2 \leq \frac{1}{\varphi}, \quad \frac{1}{\varphi^5} < \delta_4 \leq \frac{1}{\varphi^3}, \quad \frac{1}{\varphi^7} < \delta_6 \leq \frac{1}{\varphi^5}, \ \ldots. \tag{2.4}$$

-4	0	-4	-4	$\mathbf{-8}$	-12	-20	-32	-52	-84	-136	-220
-5	1	-4	-3	$\mathbf{-7}$	-10	-17	-27	-44	-71	-115	-186
-3	0	-3	-3	$\mathbf{-6}$	-9	-15	-24	-39	-63	-102	-165
-4	1	-3	-2	$\mathbf{-5}$	-7	-12	-19	-31	-50	-81	-131
-5	2	-3	-1	$\mathbf{-4}$	-5	-9	-14	-23	-37	-60	-97
-3	1	-2	-1	$\mathbf{-3}$	-4	-7	-11	-18	-29	-47	-76
-4	2	-2	0	$\mathbf{-2}$	-2	-4	-6	-10	-16	-26	-42
-5	3	-2	1	$\mathbf{-1}$	0	-1	-1	-2	-3	-5	-8
$\mathbf{-3}$	$\mathbf{2}$	$\mathbf{-1}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{5}$	$\mathbf{8}$	$\mathbf{13}$
-4	3	-1	2	$\mathbf{1}$	3	4	7	11	18	29	47
-2	2	0	2	$\mathbf{2}$	4	6	10	16	26	42	68
-3	3	0	3	$\mathbf{3}$	6	9	15	24	39	63	102
-4	4	0	4	$\mathbf{4}$	8	12	20	32	52	84	136
-2	3	1	4	$\mathbf{5}$	9	14	23	37	60	97	157
-3	4	1	5	$\mathbf{6}$	11	17	28	45	73	118	191
-1	3	2	5	$\mathbf{7}$	12	19	31	50	81	131	212
-2	4	2	6	$\mathbf{8}$	14	22	36	58	94	152	246

FIGURE 1. The Wythoff array.

In other words, a pair of integers (m, n), not both zero, appear as consecutive, positively indexed terms of a Fibonacci sequence precisely when $-1 \leq n - m\varphi \leq \frac{1}{\varphi}$. This fact supplies a neat explanation of one of the most striking features of the Wythoff array.

Theorem 2.3. *With the exceptions of* 0 *and* -1*, every integer appears exactly once in the portion of the Wythoff array consisting of columns two and greater.*

Proof. A given integer n occurs within this part of the array once for each integer m such that (m, n) are consecutive, positively indexed terms within some Fibonacci sequence. As demonstrated above, we obtain such a pair for each integer m satisfying $-1 \leq n - m\varphi \leq \frac{1}{\varphi}$. Rearranging gives

$$\frac{n}{\varphi} - \frac{1}{\varphi^2} \leq m \leq \frac{n}{\varphi} + \frac{1}{\varphi}. \tag{2.5}$$

Therefore m is confined to a closed interval of length one. Hence, in general there will be a unique integral solution for m, unless the endpoints of the interval are integers. This occurs when $\frac{1}{\varphi}(n+1) \in \mathbb{Z}$, which is only possible for $n = -1$, in which case there are two solutions for m. The only other exception arises when $n = 0$, since the corresponding solution is $m = 0$, giving the only pair of values we must avoid. In summary, every integer n appears exactly once to the right of the vertical bar in Figure 1 except for -1, which occurs twice, and 0, which is missing. □

As indicated earlier, these results, aside from the technique for locating pairs (m, n) within the Wythoff array, are known (see [13] or [8]); however, the sequence of ideas and method of proof are new.

3. The Norm of a Fibonacci Sequence

Let us say that a prime p divides a certain Fibonacci sequence if that sequence contains a multiple of p. For instance, it is known that 7 divides every Fibonacci sequence. Certain other

primes, such as 13, 17, 29, 37, and 41, seem to divide only half of all such sequences. Our purpose in this section is to define an integer associated with a Fibonacci sequence, called the norm, that will provide a means for ascertaining which sequences are divisible by primes such as the ones just listed.

Given a Fibonacci sequence generated by a_0 and $a_1 = \lfloor (a_0+1)\varphi \rfloor$, one may solve the recurrence $a_{k+1} = a_k + a_{k-1}$ to obtain the closed-form expression

$$a_k = \frac{\alpha\varphi^k - \overline{\alpha}\,\overline{\varphi}^k}{\sqrt{5}}, \qquad \alpha = a_1 - a_0\overline{\varphi}, \tag{3.1}$$

where $\overline{\varphi} = \frac{1}{2}(1-\sqrt{5})$ and α has conjugate $\overline{\alpha} = a_1 - a_0\varphi$. Note that $\overline{\alpha}\,\overline{\varphi}^k = \delta_0(-\frac{1}{\varphi})^k = \delta_k$, so (3.1) may be recast as $a_k = \frac{1}{\sqrt{5}}(\overline{\delta}_k - \delta_k)$, which makes sense considering $\delta_k = a_{k+1} - a_k\varphi$.

Each $\alpha \in \mathbb{Z}[\varphi]^*$ gives rise to a Fibonacci sequence via (3.1). Recall that the ring

$$\mathbb{Z}[\varphi] = \{c + d\varphi \mid c, d \in \mathbb{Z}\} \tag{3.2}$$

is a unique factorization domain having units $\pm\varphi^k$ for $k \in \mathbb{Z}$. Its nonzero elements $\mathbb{Z}[\varphi]^*$ form a multiplicative group having subgroup $B = \{\varphi^k \mid k \in \mathbb{Z}\}$. Replacing α by $\alpha\varphi^k$ amounts to simply reindexing the sequence corresponding to α, so we have a bijection between the elements of $\mathbb{Z}[\varphi]^*/B$ and the set of all Fibonacci sequences.

With these preliminaries in mind, we define the norm of the Fibonacci sequence given by $a_k = \frac{1}{\sqrt{5}}(\alpha\varphi^k - \overline{\alpha}\,\overline{\varphi}^k)$, indexed according to our convention, to be $N = \alpha\overline{\alpha}$. Since $\overline{\alpha} = \delta_0$ we have

$$N = \alpha\overline{\alpha} = \delta_0\overline{\delta}_0 = a_1^2 - a_1a_0 - a_0^2. \tag{3.3}$$

Therefore the norm of row r of the Wythoff array is

$$N = \lfloor (r+1)\varphi \rfloor^2 - r\lfloor (r+1)\varphi \rfloor - r^2. \tag{3.4}$$

The manner in which we index a sequence affects the sign of the norm, since shifting the numbering by one place gives norm $(\alpha\varphi)(\overline{\alpha}\,\overline{\varphi}) = -\alpha\overline{\alpha} = -N$.

We remark that the norm is positive for rows $r \geq 0$ and negative when $r < 0$. This occurs because the final expression in (3.3) will be positive when $a_1 > a_0\varphi$, which is easily shown to be the case for $r \geq 0$ since

$$\lfloor (r+1)\varphi \rfloor > (r+1)\varphi - 1 = r\varphi + (\varphi - 1) > r\varphi. \tag{3.5}$$

In a similar fashion one finds that the norm is negative when $r < 0$. Thus the sign of the norm agrees with the eventual sign of the terms of a Fibonacci sequence. We also observe that the magnitude of the norm may be found from any two consecutive terms of a Fibonacci sequence by computing $|a_{k+1}^2 - a_ka_{k+1} - a_k^2|$. This is so because

$$|a_{k+1}^2 - a_ka_{k+1} - a_k^2| = |\delta_k\overline{\delta}_k| = \left|\delta_0\overline{\delta}_0\frac{1}{(\varphi\overline{\varphi})^k}\right| = |\overline{\alpha}\alpha| = |N|. \tag{3.6}$$

For instance, $2013^2 - 2013 \cdot 1492 - 1492^2 = -1177291$. Hence the norm of the row containing 1492 and 2013 as consecutive terms is ± 1177291. This observation also demonstrates the equivalence of our definition of the norm of a Fibonacci sequence with that of the "D-value" given in [1].

The norm measures how well the ratios of consecutive terms within a Fibonacci sequence come to approximating the golden ratio by comparing the difference between $\frac{a_{k+1}}{a_k}$ and φ with

the square of the denominator a_k. More precisely, we are led to consider the product

$$a_k^2 \left| \frac{a_{k+1}}{a_k} - \varphi \right| = a_k |a_{k+1} - a_k \varphi|. \tag{3.7}$$

Proposition 3.1. *Let $\{a_k\}_{k\in\mathbb{Z}}$ be the Fibonacci sequence given by $a_k = \frac{1}{\sqrt{5}}(\alpha\varphi^k - \overline{\alpha}\,\overline{\varphi}^k)$. Then we have*

$$\lim_{k\to\infty} \sqrt{5}\, a_k \langle a_k \varphi \rangle = N, \tag{3.8}$$

where $\langle x \rangle$ is the distance from x to the nearest integer and $N = \alpha\overline{\alpha}$.

Proof. Since $\delta_k = a_{k+1} - a_k\varphi$ and $\delta_k = (-\frac{1}{\varphi})^k \delta_0 \to 0$, we know that from some point onward the integer nearest to $a_k\varphi$ is a_{k+1}. Therefore for these k we have

$$\langle a_k \varphi \rangle = |a_{k+1} - a_k\varphi| = |\delta_k| = \left| \frac{\delta_0}{\varphi^k} \right|. \tag{3.9}$$

But $\frac{1}{\varphi} < \delta_0 \leq \varphi$, so δ_0 is always positive. Using (3.1) and the fact that $\delta_0 = \overline{\alpha}$ we find that for k sufficiently large

$$\sqrt{5}\, a_k \langle a_k \varphi \rangle = (\alpha\varphi^k - \overline{\alpha}\,\overline{\varphi}^k) \cdot \frac{\overline{\alpha}}{\varphi^k} = \alpha\overline{\alpha} - \left(-\frac{1}{\varphi^2}\right)^k \overline{\alpha}^2. \tag{3.10}$$

Thus taking the limit as $k \to \infty$ gives N, as desired. □

Finally, we introduce one further notion based upon the norm that is necessary to make accurate our observation regarding certain primes dividing half of all Fibonacci sequences. We say that a Fibonacci sequence with norm N is regular $\bmod p$ when $N \not\equiv 0 \pmod{p}$. Equivalently, the Fibonacci sequence $\{a_k\}$ is regular $\bmod p$ if and only if it satisfies the second-order recursion $a_{k+2} \equiv a_{k+1} + a_k \pmod{p}$, but does not satisfy any lower-order recursion $\bmod p$. One can show that $\{a_k\}$ is irregular $\bmod p$ precisely when either $a_0 \equiv a_1 \equiv 0 \pmod{p}$, so that $\{a_k\}$ is the trivial Fibonacci sequence $\bmod p$, or it is the case that φ and $\overline{\varphi}$ are both elements of $\mathbb{Z}/p\mathbb{Z}$ and either $a_1 \equiv a_0\phi \pmod{p}$ or $a_1 \equiv a_0\overline{\varphi} \pmod{p}$. The significance of these facts is that if $a_0 \not\equiv 0 \pmod{p}$, then p is not a divisor of $\{a_k\}$ when $\{a_k\}$ is irregular $\bmod p$. The definition of regular second-order linear recurrences $\bmod p$ is given in [7].

4. Preliminary Results

Our next task is to precisely describe primes such as 13, 17, 29, 37, and 41 that divide only half of all regular Fibonacci sequences $\bmod p$. It is well-known (see [11]) that a given prime p divides F_h, where $h = p - \left(\frac{5}{p}\right)$. Suppose that g is the smallest positive integer for which $F_g \equiv 0 \pmod{p}$; i.e. g is the rank of appearance of p in the Fibonacci sequence. Then $g \,|\, h$ and we define the Fibonacci index of p as $\mathrm{ind}_F(p) = \frac{h}{g}$. The set of primes that will concern us are those with $\mathrm{ind}_F(p) = 2$. Thus $\mathrm{ind}_F(17) = 2$ since $F_9 = 34$ is the first multiple of 17, while $17 - \left(\frac{5}{17}\right) = 18$, so $g = 9$ while $h = 18$.

We will ultimately show that a prime p with $\mathrm{ind}_F(p) = 2$ divides a Fibonacci sequence of norm N precisely when N is a nonzero square $\bmod p$ or every term is divisible by p. We begin by presenting several preliminary notions and results. Recall that in the ring $\mathbb{Z}[\varphi]$ an integer prime p splits as a product $p = \pi\overline{\pi}$ of two primes when $p \equiv \pm 1 \pmod{5}$ while it is inert (remains prime) in $\mathbb{Z}[\varphi]$ when $p \equiv \pm 2 \pmod{5}$. In the former case there are p distinct congruence classes $\bmod \pi$. Given $\alpha \not\equiv 0 \pmod{\pi}$ the order of α is the least positive integer n for which $\alpha^n \equiv 1 \pmod{\pi}$, denoted $\mathrm{ord}_\pi(\alpha) = n$, and the index of α is the integer

$\text{ind}_\pi(\alpha) = \frac{1}{n}(p-1)$. In the latter case there are p^2 congruence classes $\bmod p$. The order $\text{ord}_p(\alpha) = n$ is defined similarly and $\text{ind}_p(\alpha) = \frac{1}{n}(p^2-1)$.

Proposition 4.1. *We have* $\text{ind}_\pi(-\varphi^2) = \text{ind}_F(p)$ *and* $\text{ord}_\pi(-\varphi^2) = (p-1)/\text{ind}_F(p)$ *when* $p = \pi\overline{\pi} \equiv \pm 1 \bmod 5$, *while* $\text{ind}_p(-\varphi^2) = (p-1)\text{ind}_F(p)$ *and* $\text{ord}_p(-\varphi^2) = (p+1)/\text{ind}_F(p)$ *when* $p \equiv \pm 2 \pmod 5$.

Proof. To begin, assume that $p \equiv \pm 1 \pmod 5$ with $p = \pi\overline{\pi}$ and suppose that $F_k \equiv 0 \pmod p$, so that

$$\frac{1}{\sqrt{5}}(\varphi^k - \overline{\varphi}^k) \equiv 0 \pmod \pi. \tag{4.1}$$

Note that $\sqrt{5} = \varphi - \overline{\varphi} \in \mathbb{Z}[\varphi]$ and that $\sqrt{5} \not\equiv 0 \pmod \pi$. Multiplying by $(-\varphi)^k\sqrt{5}$ and rearranging then gives $(-\varphi^2)^k \equiv 1 \pmod \pi$. These steps are reversible, using the fact that rational integers congruent $\bmod \pi$ are also congruent $\bmod p$. Therefore the smallest index g with $F_g \equiv 0 \pmod p$ matches the smallest n for which $(-\varphi^2)^n \equiv 1 \pmod \pi$. Since $h = p-1$ we conclude that $\text{ind}_\pi(-\varphi^2) = \frac{1}{n}(p-1) = \frac{h}{g} = \text{ind}_F(p)$. The argument is nearly identical in the case $p \equiv \pm 2 \pmod 5$, except that now $h = p+1$ and we finish by stating that $\text{ind}_p(-\varphi^2) = \frac{1}{n}(p^2-1) = (p-1)\frac{h}{g} = (p-1)\text{ind}_F(p)$. The formulas for the order of $(-\varphi^2)$ follow immediately from the definition. □

Proposition 4.2. *Let* p *be a prime with* $p \equiv \pm 2 \pmod 5$ *and take any element* $\alpha \in \mathbb{Z}[\varphi]^*$. *Then* $\alpha^{p+1} \equiv N \pmod p$, *where* $N = \alpha\overline{\alpha}$. *In particular,* $\varphi^{p+1} \equiv -1 \pmod p$.

Proof. Write $\alpha = c + d\varphi$, and note that p is a prime in $\mathbb{Z}[\varphi]$. Using the binomial expansion and Fermat's Little Theorem we see that

$$\alpha^p \equiv c^p + d^p\varphi^p \equiv c + d\varphi^p \pmod p. \tag{4.2}$$

We next use the fact that $\varphi^p = F_{p-1} + F_p\varphi$. When $p \equiv \pm 2 \pmod 5$ it follows from [9, p. 192–193] that $F_{p-1} \equiv 1 \pmod p$ while $F_p \equiv -1 \pmod p$. Therefore,

$$\alpha^p \equiv c + d(1-\varphi) \equiv c + d\overline{\varphi} \equiv \overline{\alpha} \pmod p. \tag{4.3}$$

It follows that $\alpha^{p+1} \equiv \alpha\overline{\alpha} \equiv N \pmod p$. □

Proposition 4.3. *If* p *is a prime for which* $\text{ind}_F(p) = 2$ *then* $p \equiv 1 \pmod 4$.

Proof. We will handle $p \equiv \pm 1 \pmod 5$ and $p \equiv \pm 2 \pmod 5$ separately. In the former case write $p = \pi\overline{\pi}$ in $\mathbb{Z}[\varphi]$. We know that $\text{ord}_\pi(-\varphi^2) = \frac{1}{2}(p-1)$ by Proposition 4.1, so

$$1 \equiv (-\varphi^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}\varphi^{p-1} \pmod \pi. \tag{4.4}$$

But $\varphi^{p-1} \equiv 1 \pmod \pi$, so $(-1)^{(p-1)/2} \equiv 1 \pmod \pi$ also, which forces $p \equiv 1 \pmod 4$.

In the same fashion, when $p \equiv \pm 2 \pmod 5$ we have $\text{ord}_p(-\varphi^2) = \frac{1}{2}(p+1)$, so

$$1 \equiv (-\varphi^2)^{(p+1)/2} \equiv (-1)^{(p+1)/2}\varphi^{p+1} \pmod p. \tag{4.5}$$

By Proposition 4.2 we know that $\varphi^{p+1} \equiv -1 \pmod p$, hence, $(-1)^{(p+1)/2} \equiv -1 \pmod p$ as well, which once again requires $p \equiv 1 \pmod 4$. (It is possible for $1 \equiv -1 \pmod p$ when $p = 2$, but $\text{ind}_F(2) = 1$, so this exception does not arise.) This completes the proof. □

Note that Proposition 4.3 is well-known; see for example [3] or [11]. For the sake of completeness we have included a proof here.

5. Determining Divisibility

We are now prepared to state and prove our main result.

Theorem 5.1. *Let p be a prime for which $\operatorname{ind}_F(p) = 2$. Then p divides a Fibonacci sequence with norm N if and only if N is a nonzero square $\bmod p$ or every term of the sequence is divisible by p.*

Proof. Since $\operatorname{ind}_F(5) = 1$ we need only consider $p \equiv \pm 1 \pmod 5$ and $p \equiv \pm 2 \pmod 5$. In the former case write $p = \pi\overline{\pi}$ and suppose that p divides the term a_k in the Fibonacci sequence given by $a_k = \frac{1}{\sqrt{5}}(\alpha\varphi^k - \overline{\alpha}\,\overline{\varphi}^k)$. Reducing mod π leads to

$$\alpha\varphi^k \equiv \overline{\alpha}\,\overline{\varphi}^k \pmod{\pi}. \tag{5.1}$$

Multiplying through by $\alpha(-\varphi)^k$ we obtain

$$\alpha^2(-\varphi^2)^k \equiv \alpha\overline{\alpha} \equiv N \pmod{\pi}. \tag{5.2}$$

By Proposition 4.1 we know that $\operatorname{ord}_\pi(-\varphi^2) = \frac{1}{2}(p-1)$. Therefore raising both sides of the above equality to the power $\frac{1}{2}(p-1)$ gives

$$N^{(p-1)/2} \equiv \alpha^{p-1} \pmod{\pi}. \tag{5.3}$$

Now if $\alpha \not\equiv 0 \pmod\pi$ then $\alpha^{p-1} \equiv 1 \pmod\pi$ and we deduce that $N^{(p-1)/2} \equiv 1 \pmod p$, hence $(\frac{N}{p}) = 1$ and N is a nonzero square $\bmod p$. On the other hand, if $\alpha \equiv 0 \pmod\pi$ then (5.1) shows that $\overline{\alpha} \equiv 0 \pmod\pi$ as well; therefore $a_k \equiv 0 \pmod\pi$, and thus $\bmod p$, for all k.

Conversely, if all terms of a certain Fibonacci sequence are divisible by p then we are done, so suppose that the norm N is a nonzero square mod p. Thus, $N \equiv b^2 \pmod p$, which reduces to $\alpha\overline{\alpha} \equiv b^2 \pmod\pi$. Dividing by α^2 yields

$$\frac{\overline{\alpha}}{\alpha} \equiv \left(\frac{b}{\alpha}\right)^2 \pmod{\pi}. \tag{5.4}$$

Since $\operatorname{ind}_\pi(-\varphi^2) = 2$ we know powers of $-\varphi^2$ give all squares $\bmod \pi$, thus

$$\frac{\overline{\alpha}}{\alpha} \equiv (-\varphi^2)^k \pmod{\pi} \tag{5.5}$$

for some positive integer k. Multiplying through by $\alpha\overline{\varphi}^k$ gives $\overline{\alpha}\,\overline{\varphi}^k \equiv \alpha\varphi^k \pmod\pi$, which leads to $a_k \equiv 0 \pmod p$ as above. Therefore p divides this Fibonacci sequence.

Now take $p \equiv \pm 2 \pmod 5$ instead so that p is prime in $\mathbb{Z}[\varphi]$, and suppose that p divides the term $a_k = \frac{1}{\sqrt{5}}(\alpha\varphi^k - \overline{\alpha}\,\overline{\varphi}^k)$. Rearranging as usual brings us to

$$\alpha^2(-\varphi^2)^k \equiv \alpha\overline{\alpha} \equiv N \pmod{p}. \tag{5.6}$$

This time we raise both sides to the power $\frac{1}{2}(p+1)$ to obtain

$$\alpha^{p+1}[(-1)^{(p+1)/2}\varphi^{p+1}]^k \equiv N^{(p+1)/2} \pmod{p}. \tag{5.7}$$

If $\alpha \equiv 0 \pmod p$ then we may conclude that every term of the sequence is divisible by p in the same manner as before. So assume that $\alpha \not\equiv 0 \pmod p$, meaning that $N \not\equiv 0 \pmod p$ either. Then Propositions 4.2 and 4.3 enable us to simplify (5.7) to

$$N \equiv N^{(p+1)/2} \pmod{p}, \tag{5.8}$$

or $N^{(p-1)/2} \equiv 1 \pmod p$. Therefore $(\frac{N}{p}) = 1$ and N is again a nonzero square $\bmod p$.

As before, to establish the converse we need only consider the case in which N is a nonzero square mod p. This implies that $N^{(p-1)/2} \equiv 1 \pmod{p}$. By Proposition 4.2 we know $N \equiv \alpha^{p+1} \pmod{p}$ in $\mathbb{Z}[\varphi]$, giving

$$\alpha^{(p^2-1)/2} \equiv 1 \pmod{p}. \tag{5.9}$$

We wish to show that $\frac{\overline{\alpha}}{\alpha}$ is a power of $(-\varphi^2)$ in order to finish as above. By Proposition 4.1 we know $\text{ord}_p(-\varphi^2) = \frac{1}{2}(p+1)$, so it suffices to show that $(\frac{\overline{\alpha}}{\alpha})^{(p+1)/2} \equiv 1 \pmod{p}$. We compute

$$\left(\frac{\overline{\alpha}}{\alpha}\right)^{(p+1)/2} \equiv \frac{(\alpha^p)^{(p+1)/2}}{\alpha^{(p+1)/2}} \equiv \alpha^{(p-1)(p+1)/2} \equiv 1, \tag{5.10}$$

using (5.9) and the fact that $\overline{\alpha} \equiv \alpha^p \pmod{p}$ from the proof of Proposition 4.2. Hence, $\frac{\overline{\alpha}}{\alpha} \equiv (-\varphi^2)^k \bmod p$ for some k, which means that $a_k \equiv 0 \pmod{p}$. Therefore p divides this Fibonacci sequence, and the entire proof is complete. □

We also outline an alternate approach to proving Theorem 5.1 based on equivalence classes of Fibonacci sequences mod p. Two Fibonacci sequences are equivalent mod p if one sequence is a nonzero multiple of a translation of the other sequence mod p. Now suppose that a prime p has a Fibonacci index of 2, so that $g = \frac{1}{2}\big(p - \big(\frac{5}{p}\big)\big)$. Then there are exactly two equivalence classes of regular Fibonacci sequences mod p. Moreover, by Proposition 4.3, we know that $p \equiv 1 \pmod{4}$. By the argument given in [12], if the Fibonacci sequence $\{a_k\}$ is in the same equivalence class as $\{b_k\}$, then the Legendre symbols with respect to p of their respective norms have the same value. Clearly every prime p is a divisor of $\{F_k\}$ since $F_0 = 0$. Moreover, the norm of the Fibonacci sequence is 1, which implies that $\{F_k\}$ is regular mod p for all primes p. It now follows that p is a divisor of a regular Fibonacci sequence $\{a_k\} \pmod{p}$ if and only if $\{a_k\}$ is equivalent to $\{F_k\} \pmod{p}$. By[16], if g is odd, then the Lucas sequence $\{L_k\}$ is regular mod p and is not in the same equivalence class as $\{F_k\}$, while if g is even, then the Fibonacci sequence $\{t_k\}$ is regular mod p and is not in the same equivalence class as $\{F_k\}$, where $t_0 = 1$, $t_1^2 \equiv -1 \pmod{p}$, and $1 \le t_1 \le \frac{1}{2}(p-1)$. Noting that $\{F_k\}$ has norm equal to 1 and $\big(\frac{1}{p}\big) = 1$ for all p, it suffices to show that if g is odd and $N_L = 5$ is the norm of $\{L_k\}$, then $\big(\frac{N_L}{p}\big) = -1$, while if g is even and $N_t = |-2-t_1|$ is the norm of $\{t_k\}$, then $\big(\frac{N_t}{p}\big) = -1$. The result for N_L is proved in [12], while the result for N_t follows from [15] and Proposition 4.3.

6. Concluding Remarks

Although it is true that $p^2 \mid N$ when every term of a Fibonacci sequence is divisible by p, one cannot restate Theorem 5.1 in these terms because the value of N does not identify which sequences are divisible by p when $N \equiv 0 \pmod{p}$. Take $p = 11$, for example. The sequences beginning $0, 11, 11, 22, \ldots$ and $7, 17, 24, 41, \ldots$ both have norm $N = 121$, but only the former sequence is divisible by 11. This remark does not apply when $p \equiv \pm 2 \pmod{5}$, since p remains prime in $\mathbb{Z}[\varphi]$ one can show that if $p^2 \mid N$ then $\alpha, \overline{\alpha} \equiv 0 \pmod{p}$, making all terms of the sequence multiples of p. Furthermore, observe that since the norm $N = 121$ of the sequence $7, 17, 24, 41, \ldots$ is a perfect square, it follows from Theorem 5.1 that this sequence is divisible by every prime of index two. (Note that $\text{ind}_F(11) = 1$, so these observations are not contradictory.)

To illustrate the main result we return to the Fibonacci sequence having consecutive terms 1492 and 2013 and ask whether any term is divisible by 2017. (We chose 2017 because it is a prime with $\text{ind}_F(2017) = 2$.) Recall that the sign of the norm depends on the indexing, so at best we know $|N| = |2013^2 - 1492 \cdot 2013 - 1492^2| = 1177291$. But according to Proposition

4.3, primes with $\mathrm{ind}_F(p) = 2$ satisfy $p \equiv 1 \pmod 4$, so the value of $(\frac{N}{p})$ does not depend on the sign of N. Therefore we compute $(\frac{1177291}{2017}) = -1$, allowing us to conclude that no term of the Fibonacci sequence containing consecutive terms 1492 and 2013 is divisible by 2017.

Finally, we indicate how these methods extend to primes for which $\mathrm{ind}_F(p) \neq 2$. The following result was proved by Catlin in [5]; an explanation can also be given that proceeds along the same lines as those of Theorem 5.1.

Theorem 6.1. *Let $\{a_k\}$ be a Fibonacci sequence with norm N and let p be a prime for which $\mathrm{ind}_F(p) = 1$. Then p is a divisor of $\{a_k\}$ if and only if $p \nmid N$ or it is the case that $p \mid a_0$ and $p \mid a_1$. Moreover, if p exactly divides N, then p is not a divisor of $\{a_k\}$.*

We remark that $\mathrm{ind}_F(p) = 1$ only when $p = 5$ or $p \equiv 3, 7, 11, 19 \pmod{20}$. This follows from the fact that either $(-\varphi^2)^{(p-1)/2}$ or $(-\varphi^2)^{(p+1)/2}$ is not congruent to 1, using the methods of Proposition 4.3. However, this condition on p is not sufficient: we have $\mathrm{ind}_F(47) = 3$ and $\mathrm{ind}_F(211) = 5$, for instance. We also point out that the exact power of p dividing N is never odd when $p \equiv \pm 2 \pmod 5$, so those primes with $\mathrm{ind}_F(p) = 1$ divide every single Fibonacci sequence.

On the other hand, when $\mathrm{ind}_F(p) > 2$ the norm no longer, or at best only partially, distinguishes those Fibonacci sequences divisible by p. For instance, the sequences corresponding to $\alpha = (3+\varphi)(4+\varphi)$ and $\alpha = (3+\varphi)(4+\overline{\varphi})$ both have norm $N = 11 \cdot 19$, but the former is not divisible by 47 while the latter is. When $p = 61$ (the smallest prime for which $\mathrm{ind}_F(p) = 4$) it turns out that $(\frac{N}{61}) = -1$ does imply that no term is divisible by 61, but nothing can be concluded in the case $(\frac{N}{61}) = 1$. Furthermore, there is no apparent correlation between whether N is a fourth power mod 61 and whether 61 divides a Fibonacci sequence with norm N. These remarks suggest that the norm provides an effective means of determining divisibility of Fibonacci sequences by primes precisely when those primes have index 1 or 2; a set of primes having an apparent density of approximately two-thirds, according to [3].

7. Acknowledgements

The author is delighted to acknowledge the influence of his undergraduate student Brent Underwood, whose persistent and lively conversations supplied much of the motivation for the research that led to the results outlined in this paper. The author is also extraordinarily grateful to the anonymous referee for taking the time to carefully and thoroughly review this manuscript. The referee's suggestions led to a number of important improvements, including the definition of regular Fibonacci sequences mod p, the alternate approach to proving Theorem 5.1, a modification to the statement of Theorem 6.1, and several additional references.

References

[1] U. Alfred, *On the ordering of Fibonacci sequences*, The Fibonacci Quarterly, **1.1** (1963), 43–46.
[2] U. Alfred, *Primes which are factors of all Fibonacci sequences*, The Fibonacci Quarterly, **2.1** (1964), 33–38.
[3] R. Backstrom, *On the determination of the zeroes of the Fibonacci sequence*, The Fibonacci Quarterly, **4.4** (1966), 313–322.
[4] C. Ballot and M. Elia, *Rank and period of primes in the Fibonacci sequence. A trichotomy*, The Fibonacci Quarterly, **45.1** (2007), 56–63.
[5] P. Catlin, *On the divisors of second-order recurrences*, The Fibonacci Quarterly, **12.2** (1974), 175–178.
[6] C. Cooper and M. Parihar, *On primes in the Fibonacci and Lucas sequences*, J. Inst. Math. Comput. Sci. Math. Ser., **15** (2002), 115–121.
[7] W. Carlip and L. Somer, *Bounds for Frequencies of Residues of Lucas Sequences Modulo p^r*, Number Theory in Progress, Vol 2 (Zakopane-Koscielisco, 1997), 691–719, de Gruyter, Berlin, 1999.

[8] A. Fraenkel and C. Kimberling, *Generalized Wythoff arrays, shuffles and interspersions*, Discrete Math., **126** (1994), 137–149.
[9] G. H. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, sixth ed., Revised by D. Heath-Brown and J. Silverman, Oxford University Press, Oxford, 2008.
[10] M. Kôzaki and T. Nakahara, *On arithmetic properties of generalized Fibonacci sequences*, Rep. Fac. Sci. Engrg. Saga Univ. Math., **28** (1999), 17 pp.
[11] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math., **31** (1930), 419–448.
[12] H.-C. Li, *Complete and reduced residue systems of second-order recurrences modulo p*, The Fibonacci Quarterly, **38.3** (2000), 272–281.
[13] D. Morrison, *A Stolarsky Array of Wythoff Pairs*, A Collection of Manuscripts Related to the Fibonacci Sequence, The Fibonacci Association, Santa Clara, CA 1980, 134–136.
[14] L. Somer, *Which second-order linear integral recurrences have almost all primes as divisors?*, The Fibonacci Quarterly, **17.2** (1979), 111–116.
[15] L. Somer, *The divisibility properties of primary Lucas recurrences with respect to primes*, The Fibonacci Quarterly, **18.4** (1980), 316–334.
[16] L. Somer, *Upper Bounds for Frequencies of Elements in Second-Order Recurrences Over a Finite Field*, Applications of Fibonacci Numbers, Vol. 5 (St. Andrews, 1992): 527–546, Kluwer Acad. Publ., Dordrecht, 1993.
[17] M. Ward, *The prime divisors of Fibonacci numbers*, Pacific J. Math., **11** (1961), 379–386.

MSC2010: 11B39, 11R04

Department of Mathematics, Computer Science, & Statistics, St. Lawrence University, Canton, NY 13617
E-mail address: svandervelde@stlawu.edu