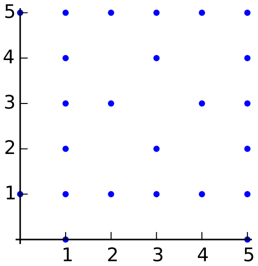
SYMMETRIES OF FIBONACCI POINTS, MOD m

PATRICK FLANAGAN, MARC S. RENAULT, AND JOSH UPDIKE

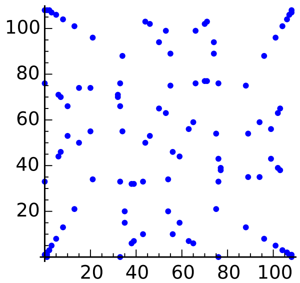
Abstract. Given a modulus m, we examine the set of all points $(F_i, F_{i+1}) \in \mathbb{Z}_m^2$ where F is the usual Fibonacci sequence. We graph the set in the fundamental domain $[0, m-1] \times [0, m-1]$, and observe that as m varies, sometimes the graph appears as a random scattering of points, but often it shows striking symmetry. We prove that in exactly three cases ($m = 2, 3, or\ 6$) the graph shows symmetry by reflection across the line $y = x$. We prove that symmetry by rotation occurs exactly when the terms $0, -1$ appear half-way through a period of $F \pmod m$. We prove that symmetry by translation can occur in essentially one way, and we provide conditions equivalent to the graph having symmetry by translation.

1. Introduction

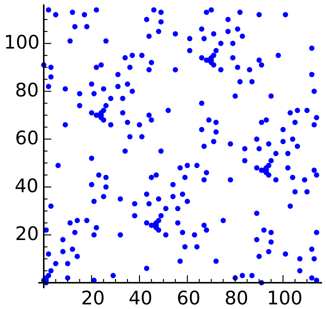
Consider points of the form $\mathbf{f}_i = \begin{bmatrix} F_i \\ F_{i+1} \end{bmatrix}$ where F is the usual Fibonacci sequence, and let $\mathcal{F} = \{\mathbf{f}_i : i \in \mathbb{Z}\}$. The sequence F, taken modulo m, is periodic and it follows that the set $\mathcal{F} \pmod m$ is finite. When we graph $\mathcal{F} \pmod m$ on the fundamental domain $[0, m-1] \times [0, m-1]$ for a variety of values of m, we see that $\mathcal{F} \pmod m$ often displays striking symmetry.



$m = 6$

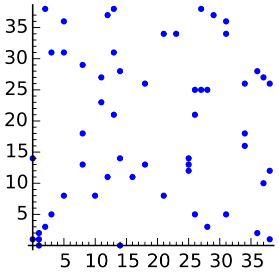


$m = 109$

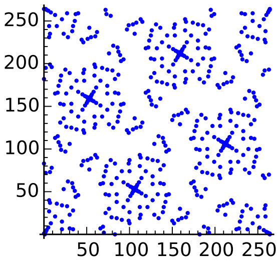


$m = 115$

For example, $\mathcal{F} \pmod 6$ displays symmetry by reflection over the line $y = x$, $\mathcal{F} \pmod{109}$ displays symmetry by rotation, and $\mathcal{F} \pmod{115}$ displays translational symmetry by four nonzero translation vectors. In fact, for m in the range $2 \leq m \leq 1000$, 166 values of m produce symmetry by translation in $\mathcal{F} \pmod m$, 263 values of m produce symmetry by rotation, and in 35 cases, both types of symmetry are present. Below we see a typical example (mod 39) where no symmetry is present and an example (mod 265) where both rotation and translation are evident.



$m = 39$



$m = 265$

In this article we describe criteria (Theorems 2.1, 3.1, and 4.3) that allow us to efficiently determine which, if any, symmetry is present in $\mathcal{F} \pmod{m}$, without having to plot all the points and look at the graph. The cases for symmetry by reflection and rotation (Theorems 2.1, 3.1, Corollary 3.2) are fairly straightforward. However, handling symmetry by translation (Lemma 4.1, Theorems 4.2, 4.3) requires significantly more care.

Of particular use in our study is the matrix $U = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ which has the property that $U^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}$. Also, $U^i \mathbf{f}_n = \mathbf{f}_{n+i}$ for any $i, n \in \mathbb{Z}$.

We let $\pi(m)$ denote the period of $F \pmod{m}$. It follows that $\pi(m)$ is also the number of points in $\mathcal{F} \pmod{m}$. Observe $U^k \mathbf{f}_n \equiv \mathbf{f}_n \pmod{m}$ if and only if $\pi(m) \mid k$. It turns out that our ability to compute $\pi(m)$ will play a key role in determining what kind of symmetry $\mathcal{F} \pmod{m}$ has. We list here some basic properties of π described by Wall [4] that allow us to compute $\pi(m)$; these results will also be useful in our proofs.

(1) If $m > 2$, then $\pi(m)$ is even.

(2) If m has prime factorization $m = \Pi p_i^{e_i}$, then $\pi(m) = \operatorname{lcm}[\pi(p_i^{e_i})]$, the least common multiple of the $\pi(p_i^{e_i})$. Two corollaries follow from this.

  (a) $\pi([m, n]) = [\pi(m), \pi(n)]$, where brackets denote least common multiple.

  (b) If $n \mid m$, then $\pi(n) \mid \pi(m)$.

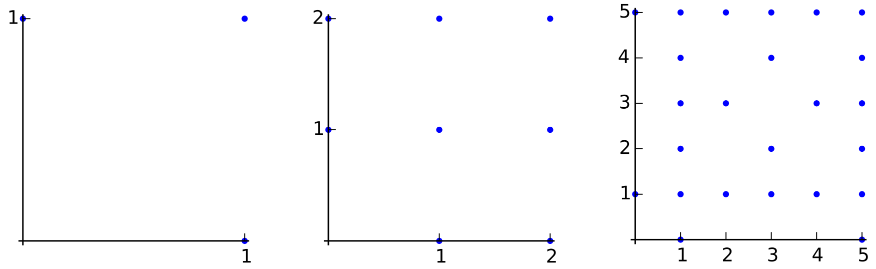
(3) If p is prime and $\pi(p) \neq \pi(p^2)$, then $\pi(p^e) = p^{e-1}\pi(p)$. (It is conjectured that $\pi(p) \neq \pi(p^2)$ for all primes.)

(4) If prime $p \equiv \pm 1 \pmod{10}$, then $\pi(p) \mid p - 1$. If $p \equiv \pm 3 \pmod{10}$, then $\pi(p) \mid 2p + 2$.

So, as long as we are capable of factoring m, we can use properties (2), (3), and (4) to easily compute $\pi(m)$. See also [1] for more on the properties of $\pi(m)$.

2. Symmetry by Reflection

We see that $\mathcal{F} \pmod{m}$ has symmetry by reflection across the line $y = x$ when $m = 2$, 3, or 6. Are there other moduli for which the graph of $\mathcal{F} \pmod{m}$ shows this kind of symmetry?



$m = 2$ $m = 3$ $m = 6$

Theorem 2.1. *$\mathcal{F} \pmod{m}$ has symmetry by reflection across the line $y = x$ exactly when $m = 2, 3,$ or 6.*

Proof. By inspection, we see $\mathcal{F} \pmod{m}$ indeed has symmetry by reflection across $y = x$ when $m = 2, 3,$ or 6.

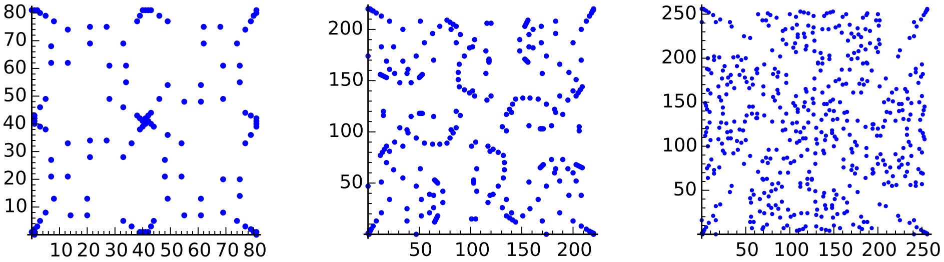
Note that $\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right] \in \mathcal{F} \pmod{m}$. Consequently, if $\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right] \notin \mathcal{F} \pmod{m}$, then we know $\mathcal{F} \pmod{m}$ does not have reflection. By inspection, we find that $\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right] \notin \mathcal{F} \pmod{m}$ for $m = 4$ or 5:

$$F \pmod{4}: \ 0, 1, 1, 2, 3, 1, 0, 1, 1, \ldots$$
$$F \pmod{5}: \ 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1 \ldots.$$

If $\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right] \in \mathcal{F} \pmod{m}$, then $U^n \equiv \left[\begin{smallmatrix}2 & 1\\1 & 3\end{smallmatrix}\right] \pmod{m}$ for some n. Comparing determinants, we find $(-1)^n \equiv 5 \pmod{m}$, but for $m \geq 7$, no n can satisfy this congruence. □

3. Symmetry by Rotation

We say that $\mathcal{F} \pmod{m}$ has symmetry by rotation if for any integer n, the point $\mathbf{f}_n$ rotated counter-clockwise one quarter turn about the origin, namely $\left[\begin{smallmatrix}0 & -1\\1 & 0\end{smallmatrix}\right] \mathbf{f}_n$, is also in $\mathcal{F} \pmod{m}$. While our definition is in terms of rotation about the origin, the repeating nature of the fundamental domain $[0, m-1] \times [0, m-1]$ in the xy-plane makes rotation appear also about the point $(\frac{m}{2}, \frac{m}{2})$.



$m = 82$ $m = 221$ $m = 257$

Theorem 3.1. *$\mathcal{F} \pmod{2}$ has symmetry by rotation. For $m > 2$, $\mathcal{F} \pmod{m}$ has symmetry by rotation if and only if $\mathbf{f}_{\frac{\pi(m)}{2}} \equiv \left[\begin{smallmatrix}0\\-1\end{smallmatrix}\right] \pmod{m}$.*

Proof. By inspection, $\mathcal{F} \pmod{2}$ has symmetry by rotation, so we may assume $m \geq 3$ and consequently, $\pi(m)$ is even.

For ease of notation, let $\pi = \pi(m)$; all congruences in this proof are taken modulo m. Assume $\mathcal{F} \pmod{m}$ has symmetry by rotation. Then, since $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right] \in \mathcal{F} \pmod{m}$, we must also have $\left[\begin{smallmatrix}-1\\0\end{smallmatrix}\right] \in \mathcal{F} \pmod{m}$. Since $U \left[\begin{smallmatrix}-1\\0\end{smallmatrix}\right] = \left[\begin{smallmatrix}0\\-1\end{smallmatrix}\right] = -\mathbf{f}_0$, we must have $-\mathbf{f}_0 \in \mathcal{F} \pmod{m}$, and so $U^n\mathbf{f}_0 \equiv -\mathbf{f}_0$ for some $0 < n < \pi$. Thus, $U^{2n}\mathbf{f}_0 \equiv U^n(-\mathbf{f}_0) \equiv \mathbf{f}_0$, and it follows that $\pi \mid 2n$. Since $0 < n < \pi$, we find $n = \pi/2$. Thus, $\mathbf{f}_{\frac{\pi}{2}} \equiv \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right]$.

Conversely, assume $\mathbf{f}_{\frac{\pi}{2}} \equiv \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right]$. We will show that for any integer n, the point $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\mathbf{f}_n$ is also in $\mathcal{F}$ (mod m). Two observations are needed. First,

$$\mathbf{f}_{-k} = \begin{bmatrix} F_{-k} \\ F_{-k+1} \end{bmatrix} = \begin{bmatrix} (-1)^{k+1}F_k \\ (-1)^k F_{k-1} \end{bmatrix} = \begin{bmatrix} 0 & (-1)^k \\ (-1)^{k+1} & 0 \end{bmatrix} \mathbf{f}_{k-1}. \tag{3.1}$$

Second, since $\mathbf{f}_{\frac{\pi}{2}} \equiv \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right]$ we get $U^{\pi/2} \equiv \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$. Thus,

$$U^{n\pi/2} \equiv \begin{bmatrix} (-1)^n & 0 \\ 0 & (-1)^n \end{bmatrix}. \tag{3.2}$$

Thus,

$$\begin{aligned}
\mathbf{f}_{n\frac{\pi}{2}-n-1} &= U^{n\pi/2}\mathbf{f}_{-n-1} \\
&= U^{n\pi/2}\begin{bmatrix} 0 & (-1)^{n+1} \\ (-1)^n & 0 \end{bmatrix}\mathbf{f}_n && \text{by (3.1), with } k = n+1 \\
&= \begin{bmatrix} 0 & (-1)^{2n+1} \\ (-1)^{2n} & 0 \end{bmatrix}\mathbf{f}_n && \text{by (3.2)} \\
&= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\mathbf{f}_n.
\end{aligned}$$

So, for any integer n, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\mathbf{f}_n \equiv \mathbf{f}_{n\frac{\pi}{2}-n-1} \in \mathcal{F}$ (mod m). □

While Theorem 3.1 does not allow us to determine whether rotation exists by analyzing only the modulus, it does give us a computationally efficient way to determine whether or not $\mathcal{F}$ (mod m) has rotation. Once we know $\pi(m)$, it is easy to determine if $U^{\pi(m)/2} \equiv \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ (mod m).

However, knowing whether or not $\mathcal{F}$ (mod m) has rotation does allow us to draw some immediate conclusions about whether or not $\mathcal{F}$ (mod n) has rotation, where n is a divisor or multiple of m.

Corollary 3.2. *If $\mathcal{F}$ (mod m) has symmetry by rotation and $n \mid m$, then $\mathcal{F}$ (mod n) also has symmetry by rotation.*

Proof. We know $\mathcal{F}$ (mod 2) has symmetry by rotation, so assume $m, n > 2$. Since $m, n > 2$ and $n \mid m$, we have $\pi(n) \mid \pi(m)$ and both periods are even. Thus, $\frac{\pi(n)}{2} \mid \frac{\pi(m)}{2}$, and so $\frac{\pi(m)}{2} = k\frac{\pi(n)}{2}$ for some integer k. Now

$$\mathbf{f}_{\frac{\pi(m)}{2}} \equiv \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right] \pmod{m} \quad \Rightarrow \quad \mathbf{f}_{\frac{\pi(m)}{2}} \equiv \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right] \pmod{n} \Rightarrow \quad \mathbf{f}_{k\frac{\pi(n)}{2}} \equiv \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right] \pmod{n}.$$

From the last congruence, k can't be even, so $k = 2t + 1$ for some integer t. Now

$$\mathbf{f}_{k\frac{\pi(n)}{2}} \equiv \mathbf{f}_{t\pi(n)+\frac{\pi(n)}{2}} \equiv \mathbf{f}_{\frac{\pi(n)}{2}} \equiv \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right] \pmod{n}$$

as needed. □

The converse of this corollary is not true. For example, both $\mathcal{F}$ (mod 5) and $\mathcal{F}$ (mod 7) exhibit rotation, but $\mathcal{F}$ (mod 35) does not.

The contrapositive of the corollary is interesting to consider: if $\mathcal{F}$ (mod m) does not show rotation, then we know that no multiple of m can produce rotation. For example, we find that $\mathcal{F}$ (mod 4) does not have rotation, and so $m \equiv 0$ (mod 4) implies $\mathcal{F}$ (mod m) does not have rotation. Here are all the values of $m < 100$ for which $\mathcal{F} \pmod{m}$ does not have rotation but for which $\mathcal{F} \pmod{n}$ does have rotation for all factors n of m:

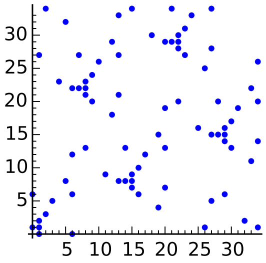
$$m = 4, 11, 15, 19, 21, 29, 31, 35, 39, 51, 59, 69, 71, 79, 91, \ldots.$$

So, modulo any multiple of any member of the above list, $\mathcal{F}$ will not exhibit rotation. For any remaining modulus less than 200, $\mathcal{F}$ will display rotation.

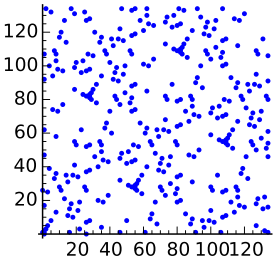
4. Symmetry by Translation

We say that $\mathcal{F} \pmod{m}$ has symmetry by translation if there is some nonzero vector $\mathbf{t} \in \mathbb{Z}_m^2$ such that for every integer i there is a corresponding integer $j(i)$ such that $\mathbf{f}_i + \mathbf{t} \equiv \mathbf{f}_{j(i)} \pmod{m}$.

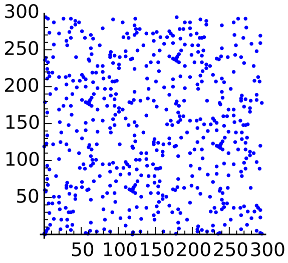
Curiously, whenever $\mathcal{F} \pmod{m}$ has symmetry by translation, there are four nonzero translations and they are multiples of $\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\3\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\4\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]$. We can see this in the three examples below.



$m = 35$



$m = 135$



$m = 295$

Lemma 4.1. *Let $\mathcal{T}$ denote the set of all translations of $\mathcal{F} \pmod{m}$. Then $\mathcal{T}$ is a group under addition and $\mathcal{T}$ is closed under left multiplication by U.*

Proof. Indeed, by virtue of what a translation is, the set of all translation is closed under addition and integer multiplication.

Of more interest to us is the fact that if $\mathbf{t}$ is a translation, then $U\mathbf{t}$ must also be a translation. If there is an index function $j(i)$ so that $\mathbf{f}_i + \mathbf{t} \equiv \mathbf{f}_{j(i)} \pmod{m}$ for all i, then $U\mathbf{f}_i + U\mathbf{t} \equiv U\mathbf{f}_{j(i)} \pmod{m}$ for all i. In other words, $\mathbf{f}_{i+1} + U\mathbf{t} \equiv \mathbf{f}_{j(i)+1} \pmod{m}$ for all i. As $\mathbf{f}_{j(i)+1} \in \mathcal{F} \pmod{m}$ for all i, we concluded $U\mathbf{t}$ is a translation. □

The following theorem shows us the form that translations must take, assuming $\mathcal{F} \pmod{m}$ has translation.

Theorem 4.2. *If $\mathcal{F} \pmod{m}$ has translation, then $5 \mid m$ and the set of all translations is $\mathcal{T} = \left\{\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right], \frac{m}{5}\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right], \frac{m}{5}\left[\begin{smallmatrix}1\\3\end{smallmatrix}\right], \frac{m}{5}\left[\begin{smallmatrix}3\\4\end{smallmatrix}\right], \frac{m}{5}\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]\right\}$.*

Proof. Assume the hypothesis and suppose that $\mathbf{t} = \left[\begin{smallmatrix}t_1\\t_2\end{smallmatrix}\right]$ is a nonzero translation of $\mathcal{F} \pmod{m}$. We begin by establishing several preliminary results.

(1) The only prime p for which $\mathcal{F} \pmod{p}$ has nonzero translation is $p = 5$.
(2) If p is prime, $p \mid m$, and $p \neq 5$, then $p \mid \mathbf{t}$.
(3) If $(t_1, t_2, m) = 1$, then $m = 5$.

We will see (1) ⇒ (2) ⇒ (3), and (3) is useful in proving the theorem.

(1) If p is prime and $\mathbf{t}$ is a nonzero translation of $\mathcal{F} \pmod{p}$, then consider the cyclic subgroup of translations generated by $\mathbf{t}$, $\langle \mathbf{t} \rangle = \{\mathbf{0}, \mathbf{t}, 2\mathbf{t}, 3\mathbf{t}, \ldots, (p-1)\mathbf{t}\}$. Now $\mathcal{F} \pmod{p}$ is a finite set with cardinality $\pi(p)$, and we can create a subset $S \subseteq \mathcal{F} \pmod{p}$ maximal with respect to the property that no point in S can be translated by a vector in $\langle \mathbf{t} \rangle$ to produce

another point in S. Then the points in S, translated under the p translations in $\langle \mathbf{t} \rangle$ result in p disjoint sets whose union is $\mathcal{F} \pmod p$. Consequently, $p \mid \pi(p)$.

It is known (see, e.g., [1] or [2]) for primes $p \equiv \pm 1 \pmod{10}$ that $\pi(p) \mid p-1$, and for primes $p \equiv \pm 3 \pmod{10}$ that $\pi(p) \mid 2p+2$. These results, combined with our observation that $p \mid \pi(p)$, show that p has neither of these forms; the only primes remaining are $p=2$ and $p=5$. By inspection, $\mathcal{F} \pmod 2$ has no nonzero translations but $\mathcal{F} \pmod 5$ does (see picture below).

(2) Suppose $\mathbf{t}$ is a nonzero translation of $\mathcal{F} \pmod m$ and there is a prime $p \neq 5$ such that $p \mid m$. Then for every integer i there is some integer $j(i)$ such that $\mathbf{f}_i + \mathbf{t} \equiv \mathbf{f}_{j(i)} \pmod m$. As $p \mid m$, this implies $\mathbf{f}_i + \mathbf{t} \equiv \mathbf{f}_{j(i)} \pmod p$ for all i, and so $\mathbf{t}$ is a translation of $\mathcal{F} \pmod p$. But $p \neq 5$, so by (1) we conclude $\mathbf{t} \equiv \mathbf{0} \pmod p$.

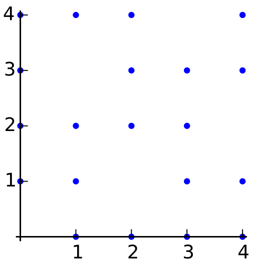
(3) Assume $\mathbf{t} = \left[\begin{smallmatrix} t_1 \\ t_2 \end{smallmatrix}\right]$ is a nonzero translation of $\mathcal{F} \pmod m$ and that $(t_1, t_2, m) = 1$. If $p \mid m$ and $p \neq 5$, then by (2), $p \mid \mathbf{t}$ so $(t_1, t_2, m) \geq p$. Thus, the only prime dividing m is 5; we conclude $m = 5^e$ for some $e \geq 1$.

Since $(t_1, t_2, 5^e) = 1$, either t_1 or t_2 is coprime to 5. Assume without loss of generality that $(t_1, 5) = 1$. (If not, then relabel $\mathbf{t}$ as $U\mathbf{t} = \left[\begin{smallmatrix} t_2 \\ t_1+t_2 \end{smallmatrix}\right]$ and note that $U\mathbf{t}$ is a translation by Lemma 4.1.) Now t_1 has an inverse modulo 5^e; let $\alpha = t_1^{-1} t_2$. Now $t_1^{-1}\mathbf{t} = \left[\begin{smallmatrix} 1 \\ \alpha \end{smallmatrix}\right] \in \mathcal{T}$. Also, $U\left[\begin{smallmatrix} 1 \\ \alpha \end{smallmatrix}\right] = \left[\begin{smallmatrix} \alpha \\ \alpha+1 \end{smallmatrix}\right] \in \mathcal{T}$, and $\alpha\left[\begin{smallmatrix} 1 \\ \alpha \end{smallmatrix}\right] = \left[\begin{smallmatrix} \alpha \\ \alpha^2 \end{smallmatrix}\right] \in \mathcal{T}$, and as a result, $\left[\begin{smallmatrix} \alpha \\ \alpha^2 \end{smallmatrix}\right] - \left[\begin{smallmatrix} \alpha \\ \alpha+1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ \alpha^2-\alpha-1 \end{smallmatrix}\right] \in \mathcal{T}$. We will show that $\alpha^2 - \alpha - 1 \equiv 0 \pmod{5^e}$. For ease of notation, let $\beta = \alpha^2 - \alpha - 1$. It is known [3] that one period of $F \pmod m$ has at most four zeros, and so there are at most four points of the form $\left[\begin{smallmatrix} 0 \\ x \end{smallmatrix}\right] \in \mathcal{F} \pmod m$. Since $\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] \in \mathcal{F} \pmod{5^e}$ and $\left[\begin{smallmatrix} 0 \\ \beta \end{smallmatrix}\right] \in \mathcal{T} \pmod{5^e}$, we see $\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 \\ \beta+1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 \\ 2\beta+1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 \\ 3\beta+1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 \\ 4\beta+1 \end{smallmatrix}\right] \in \mathcal{F} \pmod{5^e}$. Thus, among these five points, there must be a repeat. Moreover, since $\left[\begin{smallmatrix} 0 \\ -\beta \end{smallmatrix}\right] \in \mathcal{T} \pmod{5^e}$, one of the points $\left[\begin{smallmatrix} 0 \\ \beta+1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 \\ 2\beta+1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 \\ 3\beta+1 \end{smallmatrix}\right]$, or $\left[\begin{smallmatrix} 0 \\ 4\beta+1 \end{smallmatrix}\right]$ is congruent to $\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] \pmod{5^e}$. Consequently, either $\beta, 2\beta, 3\beta$, or 4β is congruent to $0 \pmod{5^e}$. In all of these cases, we can conclude $\beta \equiv 0 \pmod{5^e}$. The congruence $\alpha^2 - \alpha - 1 \equiv 0$ has a solution modulo 5 (namely, $\alpha \equiv 3$), but by inspection, there is no solution modulo 25. Hence, $\alpha^2 - \alpha - 1 \equiv 0 \pmod{5^e}$ has a solution only when $e = 1$. Thus, $m = 5$ as needed, and the proof of (3) is complete.

We turn now to the statement of the theorem, and assume that $\mathbf{t} = \left[\begin{smallmatrix} t_1 \\ t_2 \end{smallmatrix}\right]$ is a nonzero translation of $\mathcal{F} \pmod m$. Thus, there is some index function $j(i)$ such that $\mathbf{f}_i + \mathbf{t} \equiv \mathbf{f}_{j(i)} \pmod m$ for all $i \in \mathbb{Z}$.

Let $d = (t_1, t_2, m)$; write $\mathbf{t} = d\mathbf{t}'$ and $m = dm'$. If $m' = 1$, then $m = d$, so $\mathbf{t} = m\mathbf{t}'$. But then $\mathbf{t} \equiv \mathbf{0} \pmod m$, a contradiction. Thus, $m' \neq 1$. Since $m' \neq 1$, and $(t_1, t_2, m') = 1$, we find that $\mathbf{t} \not\equiv \mathbf{0} \pmod{m'}$. Moreover, we see $\mathbf{f}_i + \mathbf{t} \equiv \mathbf{f}_{j(i)} \pmod{m'}$, so $\mathbf{t}$ is a nonzero translation of $\mathcal{F} \pmod{m'}$.

By (3), we deduce that $m' = 5$. Thus, $5 \mid m$, and $\mathbf{t} = \frac{m}{5}\mathbf{t}'$ is a nonzero translation of $\mathcal{F} \pmod 5$.



The translations of $\mathcal{F}$ (mod 5) are $\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right], \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\3\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\4\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]$.

Since $\frac{m}{5} \not\equiv 0 \pmod 5$, it is invertible mod 5, and so $(\frac{m}{5})^{-1}\frac{m}{5}\mathbf{t}' \equiv \mathbf{t}'$ is a nonzero translation mod 5. By inspection, the nonzero translations modulo 5 are $\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\3\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\4\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]$. Thus, $\mathbf{t}' \in \{\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\3\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\4\end{smallmatrix}\right], \left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]\}$, and

$$\mathbf{t} = \frac{m}{5}\mathbf{t}' \in \left\{ \frac{m}{5}\begin{bmatrix}2\\1\end{bmatrix}, \frac{m}{5}\begin{bmatrix}1\\3\end{bmatrix}, \frac{m}{5}\begin{bmatrix}3\\4\end{bmatrix}, \frac{m}{5}\begin{bmatrix}4\\2\end{bmatrix} \right\}.$$

If $\mathbf{t}$ is any one of the above four nonzero vectors, then *all* four must be translation vectors, as the above set is equivalent to $\{\mathbf{t}, U\mathbf{t}, U^2\mathbf{t}, U^3\mathbf{t}\}$. □

By the preceding theorem, $\mathcal{F}$ (mod m) can have symmetry by translation only if m is a multiple of 5. Experimentally, it seems that for most multiples of 5, $\mathcal{F}$ (mod m) does indeed exhibit translation. Here are the multiples of 5 in the range $5 \le m \le 500$ for which $\mathcal{F}$ (mod m) does *not* have translation:

$$m = 55, 110, 155, 165, 205, 220, 305, 310, 330, 355, 385, 410, 440, 465, 495.$$

We turn now to those criteria on m that are equivalent to the existence of translation in $\mathcal{F}$ (mod m).

Theorem 4.3. *Write $m = 5^e n$ with $e \ge 0$ and $\gcd(5, n) = 1$. $\mathcal{F}$ (mod m) has translation if and only if $e \ge 1$ and $5^e \nmid \pi(n)$.*

Proof. Assume $\mathcal{F}$ (mod $5^e n$) has translation. We know from Theorem 4.2 that $e \ge 1$ and the set of all translations of $\mathcal{F}$ (mod $5^e n$) is $\mathcal{T} = \{\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right], \frac{m}{5}\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right], \frac{m}{5}\left[\begin{smallmatrix}1\\3\end{smallmatrix}\right], \frac{m}{5}\left[\begin{smallmatrix}3\\4\end{smallmatrix}\right], \frac{m}{5}\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]\}$. Let k be the least positive integer such that $\mathbf{f}_k - \mathbf{f}_0 \in \mathcal{T}$. Since $\mathcal{F}$ (mod $5^e n$) has translation, $k < \pi(5^e n)$. Modulo $5^e n$, for any $\mathbf{t} \in \mathcal{T}$ we see $U^4\mathbf{t} \equiv \mathbf{t}$, and so, $U^4(\mathbf{f}_k - \mathbf{f}_0) \equiv \mathbf{f}_k - \mathbf{f}_0$, that is, $\mathbf{f}_{k+4} - \mathbf{f}_4 \equiv \mathbf{f}_k - \mathbf{f}_0$. Thus, $\mathbf{f}_{k+4} - \mathbf{f}_k \equiv \mathbf{f}_4 - \mathbf{f}_0$. Since $\mathbf{f}_4 - \mathbf{f}_0 = \left[\begin{smallmatrix}3\\4\end{smallmatrix}\right]$, we find $U^k\left[\begin{smallmatrix}3\\4\end{smallmatrix}\right] \equiv \left[\begin{smallmatrix}3\\4\end{smallmatrix}\right]$. This tells us that the Lucas sequence $2, 1, 3, 4, \ldots$ taken modulo $5^e n$ has a period that divides k. Letting $\pi_L(m)$ denote the period of the Lucas sequence modulo m, we get $\pi_L(5^e n) \mid k$. Thus,

$$\pi_L(5^e n) < \pi(5^e n).$$

Three results due to Wall [4, Theorems 2, 9, 5] are useful to us here, and will allow us to express $\pi_L(5^e n)$ in terms of $\pi(n)$. First, $\pi(5^e n) = [\pi(5^e), \pi(n)]$ and $\pi_L(5^e n) = [\pi_L(5^e), \pi_L(n)]$. Second, $\pi_L(5^e) = \frac{1}{5}\pi(5^e)$ and $\pi_L(n) = \pi(n)$. Third, $\pi(5^e) = 4 \cdot 5^e$. Applying these results, we see

$$\pi_L(5^e n) = [\pi_L(5^e), \pi_L(n)] = \left[\frac{1}{5}\pi(5^e), \pi(n)\right] = \left[4 \cdot 5^{e-1}, \pi(n)\right].$$

Now if $5^e \mid \pi(n)$, then $[4 \cdot 5^{e-1}, \pi(n)] = [4 \cdot 5^e, \pi(n)]$, and so $\pi_L(5^e n) = \pi(5^e n)$. However, this contradicts the fact that $\pi_L(5^e n) < \pi(5^e n)$, noted earlier. Thus, $5^e \nmid \pi(n)$, as needed.

Conversely, let us assume $e \ge 1$ and $5^e \nmid \pi(n)$, and we will show that $\mathcal{F}$ (mod m) has a nonzero translation. Since $5^e \nmid \pi(n)$ we find $\pi_L(5^e n) = [4 \cdot 5^{e-1}, \pi(n)] = \frac{1}{5}[4 \cdot 5^e, \pi(n)] =$

$\frac{1}{5}\pi(5^e n)$. Let $k = \frac{1}{5}\pi(5^e n)$. With congruences taken modulo $5^e n$, we see $U^k \left[\begin{smallmatrix}3\\4\end{smallmatrix}\right] \equiv \left[\begin{smallmatrix}3\\4\end{smallmatrix}\right] \Rightarrow U^k(\mathbf{f}_4 - \mathbf{f}_0) \equiv \mathbf{f}_4 - \mathbf{f}_0 \Rightarrow \mathbf{f}_{k+4} - \mathbf{f}_k \equiv \mathbf{f}_4 - \mathbf{f}_0 \Rightarrow \mathbf{f}_{k+4} - \mathbf{f}_4 \equiv \mathbf{f}_k - \mathbf{f}_0$. Let $\mathbf{t} = \mathbf{f}_k - \mathbf{f}_0$. Observe that $\mathbf{t} \not\equiv \mathbf{0}$ and $U^4\mathbf{t} \equiv \mathbf{t}$. Also, since $k = \frac{1}{5}\pi(5^e n) = \frac{1}{5}[4 \cdot 5^e, \pi(n)]$, we see $4 \mid k$, and so $U^k\mathbf{t} \equiv \mathbf{t}$.
Claim: $\mathbf{t}$ is a translation of $\mathcal{F}$ (mod $5^e n$). We will prove the claim by showing that $\mathbf{f}_i + \mathbf{t} \equiv \mathbf{f}_{2^i k+i}$ for all $i \geq 0$.

We first observe that

$$\mathbf{f}_{rk} - \mathbf{f}_0 \equiv r\mathbf{t}, \quad r \geq 0 \tag{4.1}$$

since $\mathbf{f}_{rk} - \mathbf{f}_0 = \sum_{j=0}^{r-1}(\mathbf{f}_{jk+k} - \mathbf{f}_{jk}) = \sum_{j=0}^{r-1} U^{jk}(\mathbf{f}_k - \mathbf{f}_0) = \sum_{j=0}^{r-1}(U^k)^j\mathbf{t} \equiv \sum_{j=0}^{r-1}\mathbf{t} = r\mathbf{t}$. Since $\mathbf{f}_{5k} \equiv \mathbf{f}_0$, it also follows that $5\mathbf{t} \equiv \mathbf{0}$.

Next, observe that $U^5 = \left[\begin{smallmatrix}3 & 5\\5 & 8\end{smallmatrix}\right] = 3I + 5U$. Consequently, $U\mathbf{t} \equiv U^5\mathbf{t} = (3I + 5U)\mathbf{t} = 3\mathbf{t} + U(5\mathbf{t}) \equiv 3\mathbf{t}$. Thus,

$$U^i\mathbf{t} \equiv 3^i\mathbf{t}, \quad i \geq 0. \tag{4.2}$$

Now we have

$$\begin{aligned}
\mathbf{f}_{2^i k+i} - \mathbf{f}_i &= U^i(\mathbf{f}_{2^i k} - \mathbf{f}_0) \\
&\equiv U^i 2^i \mathbf{t} && \text{by (4.1)} \\
&\equiv 2^i 3^i \mathbf{t} && \text{by (4.2)} \\
&= 6^i\mathbf{t} \equiv \mathbf{t} && \text{since } 6\mathbf{t} \equiv \mathbf{t}.
\end{aligned}$$

Thus, $\mathbf{f}_i + \mathbf{t} \equiv \mathbf{f}_{2^i k+i}$ for all $i \geq 0$, and $\mathbf{t}$ must be a translation of $\mathcal{F}$ (mod $5^e n$). □

For example, $\mathcal{F}$ (mod 55) does not have translation since $55 = 5 \cdot 11$ and $5 \mid \pi(11) = 10$. On the other hand, $\mathcal{F}$ (mod 825) does have translation. In this case, $825 = 25 \cdot 33$, and $25 \nmid \pi(33) = 40$.

References

[1] M. S. Renault, *The Fibonacci Sequence Under Various Moduli*, Master's Thesis, Wake Forest University, 1996. `http://webspace.ship.edu/msrenault/fibonacci/FibThesis.pdf`.

[2] S. Vajda, *Fibonacci & Lucas Numbers, and the Golden Section*, Ellis Horwood Limited, Chichester, England, 1989.

[3] J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, The Fibonacci Quarterly, **1.1** (1963), 37–48.

[4] D. D. Wall, *Fibonacci series modulo m*, The American Mathematical Monthly, **67** (1960), 525–532.

MSC2010: 11B39, 11B50, 11A07

Department of Mathematics, Shippensburg University, Shippensburg, PA 17257

(corresponding author) Department of Mathematics, Shippensburg University, 1871 Old Main Drive, Shippensburg, PA 17257
E-mail address: msrenault@ship.edu

Department of Mathematics, Shippensburg University, Shippensburg, PA 17257