NOTES ON THE PISANO SEMIPERIOD

TOM HARRIS

Introduction

Fix a positive integer $m > 1$. The *modulo m Fibonacci sequence* is the sequence $f_{m,-}$ of elements of $\mathbb{Z}/m\mathbb{Z}$ defined by the recurrence:

$$f_{m,0} = 0$$
$$f_{m,1} = 1$$
$$f_{m,i+2} = f_{m,i} + f_{m,i+1}.$$

That is, $f_{m,r}$ is the class of the usual r^{th} Fibonacci number F_r taken modulo m. It is a straightforward exercise to show that this sequence is periodic for every m. We call its period the *Pisano period modulo m*, which we denote by $\pi(m)$. There is no initial segment of the sequence $f_{m,-}$ before it becomes periodic, which leads to the following formal definition.

Definition 1. The Pisano period $\pi(m)$ of an integer $m > 1$ is the least integer $r > 0$ such that $f_{m,r} = 0$ and $f_{m,r+1} = 1$.

Example 2. The Fibonacci numbers modulo 3 are:

$$0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, \ldots ; F$$

the period of this sequence is 8, so $\pi(3) = 8$.

The Pisano period is often studied using the *Fibonacci matrix* $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ considered modulo m. Since

$$P^r = \begin{pmatrix} f_{m,r-1} & f_{m,r} \\ f_{m,r} & f_{m,r+1} \end{pmatrix},$$

it follows that $\pi(m)$ is equal the order of P in $GL_2(\mathbb{Z}/m\mathbb{Z})$. The Pisano period has been studied fairly extensively, but much is still unknown about its behaviour. In section 1 we review some of the simpler known results about $\pi(m)$ together with their proofs. None of this material is original. It can be found variously in [Wal60], [Rob63], [FB92], and others.

Recently Singerman & Strudwick [SS16] have shown an application of a variant of the Pisano period to the study of Petrie polygons on quotients of the Farey map. Whereas the Pisano period $\pi(m)$ is the order of the Fibonacci matrix P in $GL_2(\mathbb{Z}/m\mathbb{Z})$, the *Pisano semiperiod* $\sigma(m)$ is the order of P in $(GL_2(\mathbb{Z}/m\mathbb{Z}))/\{\pm I\}$. This is equivalent to the following definition of $\sigma(m)$ as the period of the modulo m Fibonacci sequence *up to a sign*.

Definition 3. The Pisano semiperiod $\sigma(m)$ of an integer $m > 1$ is the least integer $r > 0$ such that $f_{m,r} = 0$ and $f_{m,r+1} = \pm 1$.

Date: September 20, 2017.

The reader can verify that if $\sigma(m) \neq \pi(m)$, then we must have $\sigma(m) = \frac{1}{2}\pi(m)$. Since $2 \equiv -1 \mod (3)$, we see in Example 2 that $\sigma(3) = 4 = \frac{1}{2}\pi(3)$. This is not always the case.

Example 4. The Fibonacci numbers modulo 11 are:

$$0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, 2, 3, \ldots;$$

the period of this sequence is 10, so $\pi(11) = 10$. The consecutive pair $0, 10$ never appears in the sequence, so $\sigma(11) = \pi(11) = 10$.

We expect the behaviour of $\sigma(m)$ to be at least as hard to determine as the behaviour of $\pi(m)$. In section 2 we study results about $\sigma(m)$ that are analogous to those results about $\pi(m)$ proven in section 1. Our main interest is in determining when $\sigma(m) = \frac{1}{2}\pi(m)$. We introduce a little terminology to describe this situation.

Definition 5. For an integer $m > 1$, we say m has *Pisano signature* -1 and write $\theta(m) = -1$ if the consecutive pair $0, -1$ (equivalently $-1, 0$) appears in the Fibonacci numbers modulo m. If this pair never occurs then we say m has *Pisano signature* 1 and write $\theta(m) = 1$.

Remark. Since $1 \equiv -1 \mod (2)$, this definition gives $\theta(2) = -1$. Instead of the above formulation we could have chosen the definition

$$\text{“}\theta(m) = -1 \textit{ if and only if } \sigma(m) = \tfrac{1}{2}\pi(m), \textit{ otherwise } \theta(m) = 1\text{”},$$

in which case $\theta(2) = 1$. Either choice leads to results whose statements have exceptions at $m = 2$, so we have made the choice that seems to lead to fewer exceptions. Away from 2 this does not present any problems, as the two formulations are equivalent for $m \neq 2$.

1. The Pisano period

In this section we review some elementary results about the Pisano period. It is often the case that some detail in the proof of a result about $\pi(m)$ yields a a stronger result about $\sigma(m)$, so in most places we have given more detailed proofs than is strictly necessary.

Apart from the first case $\pi(2) = 3$, all Pisano periods are even. There are many proofs of this elementary fact. The following short proof is due to David Singerman.

Proposition 6. *If $m > 2$, then $\pi(m)$ is even.*

Proof. We have seen that $\pi(m)$ is equal the order of $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ in $GL_2(\mathbb{Z}/m\mathbb{Z})$. Considering the determinant homomorphism $\det\colon GL_2(\mathbb{Z}/m\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})^\times$, we see that $\det(P) = -1$, so $(-1)^{\pi(m)} = 1$ in $\mathbb{Z}/m\mathbb{Z}$. Since $m \neq 2$, we have $-1 \neq 1$ in $\mathbb{Z}/m\mathbb{Z}$, so $\pi(m)$ must be even. □

The following lemma is a direct application of the Chinese remainder theorem.

Lemma 7. *Let m_1, m_2 be coprime. Then $\pi(m_1 m_2) = \operatorname{lcm}(\pi(m_1), \pi(m_2))$.*

Proof. Since m_1 and m_2 are coprime, the Chinese remainder theorem tells us that:

$$\begin{aligned} F_r \equiv 0 \mod (m) &\iff F_r \equiv 0 \mod (m_i), \quad i = 1, 2 \\ \text{and} \quad F_{r+1} \equiv 1 \mod (m) &\iff F_r \equiv 1 \mod (m_i), \quad i = 1, 2. \end{aligned}$$

Thus $f_{m,r} = 0$ and $f_{m,r+1} = 1$ when $r = \operatorname{lcm}(\pi(m_1), \pi(m_2))$, and not before. So $\pi(m_1 m_2) = \operatorname{lcm}(\pi(m_1), \pi(m_2))$. □

The least common multiple is associative, so it follows that for mutually coprime $m_1, \ldots, m_r$ we have $\pi(m_1 m_2 \cdots m_r) = \operatorname{lcm}(\pi(m_1), \pi(m_2), \ldots, \pi(m_r))$ This is also proven directly by the same argument as above.

So the calculation of $\pi(m)$ reduces trivially to the calculation of $\pi(p^e)$ for p a prime. The picture for prime powers is more complicated. The following conjecture is widely expected to be true, and has been verified for primes up to 2.8×10^{16}, but no proof is known. Any counterexample to the conjecture would have to be a *Wall–Sun–Sun prime*. [1] No Wall–Sun–Sun primes are known to exist.

Conjecture 8. *For a prime p and an integer $e > 1$, we have $\pi(p^e) = p^{e-1}\pi(p)$.*

To establish the conjecture it is in fact enough to show that $\pi(p^2) = p\pi(p)$, as Wall already showed in 1960 that if $\pi(p^2) \neq \pi(p)$, then $\pi(p^e) = p^{e-1}\pi(p)$ (Theorem 5 of [Wal60]). In the same theorem, Wall also shows that if t is the largest integer with $\pi(p^t) = \pi(p)$, then $\pi(p^e) = p^{e-t}\pi(p)$ for $e > t$. In particular, $\pi(p^e)$ always divides $\pi(p^{e-1})$. The interested reader may prove this fact directly as an exercise.

So to find bounds on $\pi(m)$ it suffices to bound $\pi(p)$ for p prime, and to calculate $\pi(m)$ it suffices conjecturally to calculate $\pi(p)$ for primes as well. There is no known formula for $\pi(p)$, but there are effective bounds that limit the possibilities. This is not to say that it is difficult to calculate individual periods, just that the overall behaviour is not well understood.

As we have already noted, the prime 2 is an anomaly in the study of Pisano periods, having $\pi(2) = 3$ odd. Since we are dealing with series derived from the Fibonacci numbers, it should come as no surprise that $\pi(5) = 20$ is also anomalous. We will establish the reasons for this shortly. For p a prime not equal to 2 or 5, let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements, and let $\mathcal{R}_p$ be the quotient ring $\mathbb{F}_p[t]/(t^2 - t - 1)$. We denote the image of t in $\mathcal{R}_p$ by ϕ_p, and note that ϕ_p is a unit with inverse $\phi_p - 1$. By definition ϕ_p is a root of the polynomial $x^2 - x - 1 = 0$ in $\mathcal{R}_p$. We calculate also that $1 - \phi_p$ is also a root. An easy argument by induction shows that

$$\phi_p^r = f_{p,r-1} + f_{p,r}\phi_p$$

in $\mathcal{R}_p$ for $r > 0$. From the definition of the Pisano period, it now follows that $\pi(p)$ is equal to the order of ϕ_p in the group of units $\mathcal{R}_p^\times$.

Remark. We could of course define a ring $\mathcal{R}_m := (\mathbb{Z}/m\mathbb{Z})[t]/(t^2 - t - 1)$ and corresponding element ϕ_m for any $m > 1$. It remains true that $\pi(m)$ is equal to the order of ϕ_m in $\mathcal{R}_m^\times$. However the ring $\mathcal{R}_p$ is much better behaved for p prime, as $\mathbb{Z}/p\mathbb{Z}$ is a field. Since calculations of $\pi(m)$ reduce to calculations of $\pi(p^k)$ and (conjecturally) to $\pi(p)$ we do not consider the ring $\mathcal{R}_m$ for composite m here.

Proposition 9. *Let p be prime that is not 2 or 5.*

(i) If $p \equiv \pm 1 \mod (5)$, then $\pi(p)$ divides $p - 1$.
(i) If $p \equiv \pm 2 \mod (5)$, then $\pi(p)$ divides $2(p + 1)$.

[1] A prime $p \neq 2, 5$ is called a Wall–Sun–Sun prime if p^2 divides the Fibonacci number $f_{p-\left(\frac{p}{5}\right)}$, where $\left(\frac{p}{5}\right)$ is the Legendre symbol. Wall–Sun–Sun primes were originally studied in connection to potential counterexamples to Fermat's Last Theorem.

Proof. The proof goes by considering the structure of $\mathcal{R}_p$. In either case $\mathcal{R}_p$ is a commutative ring of characteristic p, so it has a Frobenius endomorphism $\mathrm{Frob}_p(a) = a^p$ which fixes all elements of the prime field $\mathbb{F}_p \subset \mathcal{R}_p$. Let $\rho(t) \in \mathbb{F}_p[t]$ be the polynomial $t^2 - t - 1$. The structure of $\mathcal{R}_p$ depends on whether or not $\rho(t)$ is irreducible in $\mathbb{F}_p[t]$. For quadratic polynomials, reducibility over a field is equivalent to having a root in the field. The class of 4 is invertible modulo odd primes, so $\rho(t) = t^2 - t - 1$ has a root in $\mathbb{F}_p$ if and only if $4t^2 - 4t - 4 = (2t-1)^2 - 5$ does. This happens whenever 5 is a quadratic residue mod p, which is case (i) where $p \equiv \pm 1 \mod (5)$ (note that in this case the two roots are distinct: for $p = 5$ there is one repeated root, which explains why 5 is anomalous). When 5 is a quadratic non-residue mod p, then we are in case (ii) where $p \equiv \pm 2 \mod (5)$.

(i) $p \equiv \pm 1 \mod (5)$: In the first case, $\rho(t)$ is reducible over $\mathbb{F}_p$, so $\rho(t) = (t-a)(t-b)$ for some distinct a and b in $\mathbb{F}_p$. Since a and b are elements of the prime field, they are fixed by the Frobenius, so they are roots of $t^p - t$. It follows that $\rho(t)$ divides $t^p - t$, so there is a containment of ideals $(t^p - t) \subset (\rho(t)) = (t^2 - t - 1)$, hence the relation $x^p = x$ holds for every element of $\mathcal{R}_p = \mathbb{F}_p[t]/(t^2 - t - 1)$. In particular we have $\phi_p^p = \phi_p$, so $\phi_p^{p-1} = 1$. Therefore the order of ϕ_p in $\mathcal{R}_p^\times$ is a divisor of $p-1$, proving the first claim.

(ii) $p \equiv \pm 2 \mod (5)$: In the second case, $\rho(t)$ is irreducible quadratic over $\mathbb{F}_p$, and therefore $\mathcal{R}_p = \mathbb{F}_p[t]/(\rho(t)) \cong \mathbb{F}_{p^2}$. Since $\mathcal{R}_p$ is a field, the only fixed points of its Frobenius are the elements of the prime subfield. We have $\phi_p^2 - \phi_p - 1 = 0$ in $\mathcal{R}_p$, so

$$\phi_p^{2p} - \phi_p^p - 1 = \mathrm{Frob}_p(\phi_p^2 - \phi_p - 1) = 0.$$

This shows that ϕ_p^p is a root of $x^2 - x - 1$ in $\mathcal{R}_p$, and so must be equal to ϕ_p or $1 - \phi_p$. But we cannot have $\phi_p^p = \phi_p$, else ϕ_p would be a fixed point of Frob_p and would have to be in the prime field, contradicting the irreducibility of $\rho(t)$. So $\phi_p^p = 1 - \phi_p$, hence

$$\phi_p^{p+1} = \phi_p - \phi_p^2 = -1,$$

and finally $\phi_p^{2(p+1)} = 1$. Therefore the order of ϕ_p in $\mathcal{R}_p^\times$ is a divisor of $2(p+1)$, proving the second claim.

□

We call primes that are of the form $p \equiv \pm 1 \mod (5)$ *reducible primes*, and those that are of the form $p \equiv \pm 2 \mod (5)$ (excluding $p = 2$) *irreducible primes*. We now have upper bounds for $\pi(p)$ in each case, more strongly we know that $\pi(p)$ divides its upper bound. We also know that 2 divides $\pi(p)$ for $p > 2$. It is clear that $\pi(p) \geq 4$ for $p > 2$. In fact we can say more: if p is an irreducible prime, then 4 *divides* $\pi(p)$. We'll derive this result as Corollary 16 from of a result about Pisano semiperiods later: the reader is invited to supply a direct proof as an exercise.

Taken together, the preceding results are enough to determine a total bound on $\pi(m)$. The proof of the following result was outlined in [FB92].

Theorem 10. *The Pisano period satisfies $\pi(m) \leq 6m$, with equality if and only if $m = 2 \cdot 5^j$ for some $j > 0$. Furthermore, if $m \neq 2 \cdot 5^j$, then $\pi(m) \leq 4m$.*

Proof. We decompose m as a product

$$m = 2^i \cdot 5^j . p_1^{e_1} \cdots p_1^{e_r} \cdot q_1^{f_1} \cdots q_s^{f_s},$$

where $p_1, \ldots, p_r$ are odd primes congruent to $\pm 2 \mod (5)$, $q_1, \ldots, q_s$ are odd primes congruent to $\pm 1 \mod (5)$. Using Lemma 7 we have

$$\pi(m) = \operatorname{lcm}(\pi(2^i \cdot 5^j \cdot p_1^{e_1} \cdots p_r^{e_r}), \pi(q_1^{f_1} \cdots q_s^{f_s})) \leq \pi(2^i \cdot 5^j \cdot p_1^{e_1} \cdots p_r^{e_r}) \cdot \pi(q_1^{f_1} \cdots q_s^{f_s}).$$

By Lemma 7 again, and the assertion following Conjecture 8 that $\pi(p^e) | p^{e-1}\pi(p)$, we have

$$\begin{aligned} \pi(q_1^{f_1} \cdots q_s^{f_s}) &= \operatorname{lcm}(\pi(q_1^{f_1}), \ldots, \pi(q_s^{f_s})) \\ &\leq \pi(q_1^{f_1}) \cdots \pi(q_s^{f_s}) \\ &\leq q_1^{f_1 - 1} \cdot \pi(q_1) \cdots q_s^{f_s - 1} \cdot \pi(q_s). \end{aligned}$$

By Proposition 9 (i), each $\pi(q_i) \leq q_j - 1$, so for products of reducible primes:

$$\pi(q_1^{f_1} \cdots q_s^{f_s}) \leq q_1^{f_1} \cdots q_s^{f_s}.$$

Therefore we can disregard reducible primes when looking for upper bounds, as

$$\frac{\pi(m)}{m} \leq \frac{\pi(2^i \cdot 5^j \cdot p_1^{e_1} \cdots p_1^{e_r})}{2^i \cdot 5^j \cdot p_1^{e_1} \cdots p_1^{e_r}}.$$

So we consider integers that are divisible only by irreducible primes, and the anomalous primes 2 and 5. It is useful to note here that $\pi(2^i) = 3 \cdot 2^{i-1}$ and $\pi(5^j) = 4 \cdot 5^j$.

First suppose that 2 does not divide m, and let $m = 5^j \cdot p_1^{e_1} \cdots p_r^{e_r}$. We have

$$\begin{aligned} \pi(5^j \cdot p_1^{e_1} \cdots p_r^{e_r}) &\leq \operatorname{lcm}(\pi(5^j), \pi(p_1^{e_1}), \ldots, \pi(p_r^{e_r})) \\ &= \operatorname{lcm}(4 \cdot 5^j, \pi(p_1^{e_1}), \ldots, \pi(p_r^{e_r})) \\ &\leq 5^j \cdot p_1^{e_1 - 1} \cdots p_r^{e_r - 1} \cdot \operatorname{lcm}(4, \pi(p_1), \ldots, \pi(p_r)), \end{aligned}$$

for the same reasons as above. From Proposition 9 (ii), each p_i divides $2(p_i + 1)$, so

$$\pi(5^j \cdot p_1^{e_1} \cdots p_r^{e_r}) \leq 5^j \cdot p_1^{e_1 - 1} \cdots p_r^{e_r - 1} \cdot \operatorname{lcm}(4, 2(p_1 + 1), \ldots, 2(p_r + 1)).$$

Furthermore, each $2(p_i + 1)$ is divisible by 4, so we have

$$\begin{aligned} \pi(p_1^{e_1} \cdots p_r^{e_r}) &\leq 4 \cdot 5^j \cdot p_1^{e_1 - 1} \cdots p_r^{e_r - 1} \cdot \operatorname{lcm}\left(\tfrac{(p_1+1)}{2}, \ldots, \tfrac{(p_r+1)}{2}\right) \\ &\leq 4 \cdot 5^j \cdot p_1^{e_1 - 1} \cdots p_r^{e_r - 1} \cdot \textstyle\prod_i \frac{p_i + 1}{2} \\ &\leq 4m \cdot \textstyle\prod_i \frac{p_i + 1}{2p_i} \\ &\leq 4m. \end{aligned}$$

The product $\prod_i \frac{p_i+1}{2}$ is always less that 1, so equality is achieved if and only if $m = 5^j$. If $m \neq 5^j$, then the maximum value of the product occurs when the only other prime involved is 3. In this case $\pi(m) \leq \frac{8}{3}m$, with equality if and only if $m = 5^j \cdot 3^k$ (here we are using $\pi(3^k) = 8 \cdot 3^{k-1}$).

Now suppose that 2 divides m, say $m = 2^i m'$ with m' coprime to 2. We note that 4 divides $\pi(m')$, since 4 divides $\pi(p)$ for any irreducible prime and 4 divides $\pi(5^j)$. We have

$$\pi(m) = \operatorname{lcm}(\pi(2^i), \pi(m')) = \operatorname{lcm}(3 \cdot 2^{i-1}, \pi(m')).$$

If $i \geq 3$, then we can divide all terms by 4 as before:

$$\begin{aligned}\pi(m) = \operatorname{lcm}(3 \cdot 2^{i-1}, \pi(m')) &= 4 \operatorname{lcm}\left(3 \cdot 2^{i-3}, \tfrac{1}{4}\pi(m')\right) \\ &\leq 4 \cdot 3 \cdot 2^{i-3} \cdot \tfrac{1}{4}\pi(m') \\ &\leq \tfrac{3}{8} \cdot 2^i \cdot 4m' \\ &= \tfrac{3}{2}m.\end{aligned}$$

If $i = 2$, then

$$\begin{aligned}\pi(m) = \operatorname{lcm}(6, \pi(m')) &= 2 \operatorname{lcm}\left(3, \tfrac{1}{2}\pi(m')\right) \\ &\leq 2 \cdot 3 \cdot \tfrac{1}{2}\pi(m') \\ &\leq 3 \cdot 4m' \\ &= 3m.\end{aligned}$$

Finally, if $i = 1$, we have

$$\begin{aligned}\pi(m) = \operatorname{lcm}(3, \pi(m')) &\leq 3\pi(m') \\ &\leq 3 \cdot 4m' \\ &= 6m.\end{aligned}$$

Since the equality $\pi(m') = 4m'$ with m' coprime to 2 is achieved only when $m' = 5^j$, it follows that $\pi(m) = 6m$ is achieved only when $m = 2 \cdot 5^j$. □

2. The Pisano semiperiod

In this section we use the results of the previous section give bounds on $\sigma(m)$ and to decide, where possible, whether $\sigma(m) = \pi(m)$ or $\frac{1}{2}\pi(m)$.

We begin our analysis of the Pisano semiperiod with a straightforward strengthening of Proposition 6.

Proposition 11. *If $m > 2$, then $\sigma(m)$ is even.*

Proof. As in the proof of Proposition 6, we have a determinant homomorphism $\det\colon GL_2(\mathbb{Z}/m\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})^\times$. Since $\det(\pm I) = 1$, the induced homomorphism

$$\overline{\det}\colon GL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm I\} \to (\mathbb{Z}/m\mathbb{Z})^\times$$

is well-defined. Recall that $\sigma(m)$ is preciely the order of the image of the Fibonacci matrix $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ in $GL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm I\}$. Then, as before, we have $\overline{\det}(P) = -1$, so $(-1)^{\sigma(m)} = 1$ in $\mathbb{Z}/m\mathbb{Z}$. As $m \neq 2$, this implies that $\sigma(m)$ is even. □

Next we attempt to mimic Lemma 7 for $\sigma(m)$. Determining the semiperiod of composite numbers *almost* reduces to determining the semiperiod of prime powers, but we are left with an ambiguous factor of 2.

Lemma 12. *Let $m_1, \ldots, m_r$ be coprime. Then $\sigma(m_1 \cdots m_r)$ is equal to one of:*

$$\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r)),$$
$$2 \operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r)).$$

Proof. Let $m = m_1 \cdots m_r$. The semiperiod $\sigma(m)$ is equal to either $\pi(m)$ or $\frac{1}{2}\pi(m)$. In either case, we have $\pi(m) = \operatorname{lcm}(\pi(m_1), \ldots, \pi(m_r))$. Each $\pi(m_i)$ is equal to either $\sigma(m_i)$ or $2\sigma(m_i)$, so the highest power of 2 occurring in the divisors of the collection $\{\pi(m_1), \ldots, \pi(m_r)\}$ can be at most one power higher than that occurring among the divisors of $\{\sigma(m_1), \ldots, \sigma(m_r)\}$. Hence $\pi(m) = \operatorname{lcm}(\pi(m_1), \ldots, \pi(m_r))$ is equal to one of

$$\begin{aligned} &\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r)), \\ &2\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r)). \end{aligned}$$

If $\sigma(m) = \pi(m)$, then this is the desired result. If $\sigma(m) = \frac{1}{2}\pi(m)$, then $\sigma(m)$ is equal to one of

$$\begin{aligned} &\tfrac{1}{2}\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r)), \\ &\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r)). \end{aligned}$$

We will show that the first of these is impossible. By definition, $\sigma(m)$ satisfies $f_{m,\sigma(m)} \equiv 0 \mod (m_1 \cdots m_r)$ and $f_{m,\sigma(m)+1} \equiv \pm 1 \mod (m_1 \cdots m_r)$. But then $f_{m,\sigma(m)} \equiv 0 \mod (m_i)$ and $f_{m,\sigma(m)+1} \equiv \pm 1 \mod (m_i)$ for $i = 1, \ldots, r$. So $\sigma(m_i)$ divides $\sigma(m)$ for each m, and therefore $\sigma(m)$ must be an integer multiple of $\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r))$, ruling out the first case. □

Two facts follow immediately from the proof of Lemma 12. Let $m = m_1 \cdots m_r$ with the m_i mutually coprime, as above. First, if $\sigma(m) = 2\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r))$, then $\theta(m) = 1$, i.e., $\sigma(m) = \pi(m)$. Second, if $\theta(m) = -1$ (i.e., $\sigma(m) = \frac{1}{2}\pi(m)$ or $m = 2$), then $\sigma(m) = \operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r))$. Furthermore, if $\theta(m_i) = -1$ for every i, then the converse is true: $\sigma(m) = \operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r))$ implies that $\theta(m) = -1$. Away from 2 we have, $\theta(m_i) = -1$ if and only if $\pi(m_i) = 2\sigma(m_i)$, so

$$\begin{aligned} \pi(m) &= \operatorname{lcm}(\pi(m_1), \ldots, \pi(m_r)) \\ &= \operatorname{lcm}(2\sigma(m_1), \ldots, 2\sigma(m_r)) \\ &= 2\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r)) \\ &= 2\sigma(m). \end{aligned}$$

Very little needs to be changed to deal with the case where some m_i is equal 2.

We now turn to the general problem of determining the Pisano signature of a product of coprime factors. Let ν_2 be the 2-adic valuation on the integers, given by defining $\nu_2(m)$ to be the largest integer a such that 2^a divides m.

Proposition 13. *Let $m_1, \ldots, m_r$ be coprime, and let $m = m_1 \cdots m_r$.*

(i) If $\theta(m_i) = 1$ for some m_i, then $\theta(m) = 1$.

(ii) If $\theta(m_i) = -1$ for every m_i, and no m_i is equal to 2, then $\theta(m) = -1$ if and only if $\nu_2(\sigma(m_1)) = \nu_2(\sigma(m_2)) = \cdots = \nu_2(\sigma(m_r))$.

(iii) If $\theta(m_i) = -1$ for every m_i, and some m_i is equal to 2 (wlog say m_1), then $\theta(m) = -1$ if and only if $\nu_2(\sigma(m_2)) = \nu_2(\sigma(m_3)) = \cdots = \nu_2(\sigma(m_r))$.

Proof. By the Chinese remainder theorem $x \equiv 0 \mod (m)$ if and only if $x \equiv 0 \mod (m_i)$ for $i = 1, \ldots, r$. Similarly $x \equiv 1 \mod (m)$ if and only if $x \equiv 1 \mod (m_i)$ for $i = 1, \ldots, r$, and $x \equiv -1 \mod (m)$ if and only if $x \equiv -1 \mod (m_i)$ for $i = 1, \ldots, r$.

(i) Suppose $\theta(m_i) = 1$ for some m_i. If $\theta(m) = -1$, then the pair $0, -1$ appears in the Fibonacci sequence modulo m. But this implies that $0, -1$ appears in the Fibonacci sequence modulo m_i, contradicting $\theta(m_i) = 1$. Hence $\theta(m) = 1$.

(ii) Suppose $\theta(m_i) = -1$ and $m_i \neq 2$ for every m_i. The statement $\theta(m_i) = -1$ is equivalent to $F_{\sigma(m)} \equiv 0 \mod (m)$ and $F_{\sigma(m)+1} \equiv -1 \mod (m)$, which is in turn equivalent to $F_{\sigma(m)} \equiv 0 \mod (m_i)$ and $F_{\sigma(m)+1} \equiv -1 \mod (m_i)$ for all i. We have $F_{k\sigma(m_i)} \equiv 0 \mod (m_i)$ and $F_{k\sigma(m_i)+1} \equiv (-1)^k \mod (m_i)$ for each i, and for every positive integer k, so $\theta(m_i) = -1$ if and only if $\sigma(m)$ is an odd multiple of each $\sigma(m_i)$. Since $\sigma(m)$ is a multiple of $\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r))$, if $\sigma(m)$ is an odd multiple of each $\sigma(m_i)$, then so is $\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r))$. Therefore $\theta(m_i) = -1$ implies that $\operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r))$ is an odd multiple of each $\sigma(m_i)$, which is equivalent to saying that all of the $\sigma(m_i)$ have the same 2-adic valuation.
Conversely, if all of the $\sigma(m_i)$ have the same 2-adic valuation, then $r = \operatorname{lcm}(\sigma(m_1), \ldots, \sigma(m_r))$ is an odd multiple of each $\sigma(m_i)$. It follows that $F_r \equiv 0 \mod (m_i)$ and $F_{r+1} \equiv -1 \mod (m_i)$ for all i. Therefore $F_r \equiv 0 \mod (m)$ and $F_{r+1} \equiv -1 \mod (m)$, and so $\theta(m) = -1$.

(iii) This is much the same as part (ii). Suppose $\theta(m_i) = -1$ for every m_i, and let $m_1 = 2$ (note that therefore $m_i \neq 2$ for $i > 1$). If $m = m_1 = 2$ the result is trivial, so let $m = 2m'$, where $m' = m_2 \cdots m_r$. We have $\theta(m) = -1$ if and only if $F_{\sigma(m)} \equiv 0 \mod (m)$ and $F_{\sigma(m)+1} \equiv -1 \mod (m)$. This is equivalent to $F_{\sigma(m)} \equiv 0 \mod (2)$, $F_{\sigma(m)+1} \equiv -1 \mod (2)$, $F_{\sigma(m)} \equiv 0 \mod (m')$, and $F_{\sigma(m)+1} \equiv -1 \mod (m')$. But $\sigma(m)$ is a multiple of $\sigma(2)$, and $F_{k\sigma(2)} \equiv 0 \mod (2)$ and $F_{k\sigma(2)+1} \equiv -1 \mod (2)$ for any positive integer k, since $1 \equiv -1 \mod (2)$. So $\theta(m) = -1$ implies $F_{\sigma(m)} \equiv 0 \mod (m')$ and $F_{\sigma(m)+1} \equiv -1 \mod (m')$, which implies $\theta(m') = -1$. Since $m' = m_2 \cdots m_r$, this implies the required condition on the 2-adic valuations of $m_2, \ldots, m_r$ by part (ii).
Conversely, the condition on the 2-adic valuations of $m_2, \ldots, m_r$ implies that $\theta(m') = -1$. Then $r = \operatorname{lcm}(\sigma(2), \sigma(m'))$ is equal to either $\sigma(m')$ or $3\sigma(m')$ (since $\sigma(2) = 3$). In either case, $F_r \equiv 0 \mod (2)$, $F_r \equiv 0 \mod (m')$, $F_r \equiv -1 \mod (2)$, and $F_r \equiv -1 \mod (m')$. This implies $F_{\sigma(m)} \equiv 0 \mod (m)$ and $F_{\sigma(m)+1} \equiv -1 \mod (m)$, $\theta(m) = -1$.

□

As a consequence of part (i) of the proposition, we can prove that asymptotically the numbers with $\theta(m) = 1$ dominate.

Having dealt with the Pisano signatures of products, we now consider the signature of primes. For the anomalous primes 2 and 5 we have $\sigma(2^i) = \pi(2^i) = 3 \cdot 2^{i-1}$, and $\sigma(5^j) = \frac{1}{2}\pi(5^j) = 2 \cdot 5^j$. The following simple lemma is a useful criterion for determining when $\theta(p) = -1$.

Lemma 14. *Let p be prime that is not 2 or 5. Then $\sigma(p) = \frac{1}{2}\pi(p)$ if and only if $-1 \in \langle \phi_p \rangle \leq \mathcal{R}_p^\times$.*

Proof. If $p \neq 2$, then $\sigma(p) = \frac{1}{2}\pi(p)$ if and only if the consecutive pair $0, -1$ appears in the Fibonacci numbers modulo m if and only the pair $-1, 0$ appears (it's the preceding pair). As we saw in section 1, in $\mathcal{R}_p$ we have

$$\phi_p^r = f_{p,r-1} + f_{p,r}\phi_p.$$

From this it is clear that the pair $-1, 0$ appears if and only if $-1 \in \langle \phi_p \rangle \leq \mathcal{R}_p^\times$. □

Remark. Lemma 14 is still true if we replace $\mathcal{R}_p$ with $\mathcal{R}_m := (\mathbb{Z}/m\mathbb{Z})[t]/(t^2-t-1)$ for any $m > 2$.

In the proof of Proposition 9 (ii) we saw that if $p \equiv \pm 2 \mod (5)$, and $p \neq 2$, then $-1 \in \langle \phi_p \rangle \leq \mathcal{R}_p^\times$. Lemma 14 therefore completely determines the relationship between σ and π for irreducible primes.

Corollary 15. *Let $p \neq 2, 5$ be prime satisfying $p \equiv \pm 2 \mod (5)$. Then $\sigma(p) = \frac{1}{2}\pi(p)$, and $\sigma(p)$ divides $p+1$.* □

From Corollary 15 we can now immediately infer the stronger result about $\pi(m)$ that was promised in the discussion following the proof of Proposition 9 (ii).

Corollary 16. *If $p \equiv \pm 2 \mod (5)$, and $p \neq 2$, then $\pi(p)$ is a multiple of 4.* □

For the remaining primes $p \equiv \pm 1 \mod (5)$ the picture is less simple. Currently we only have complete information for those p satisfying $p \equiv 11$ or $p \equiv 19 \mod (20)$.

Proposition 17. *Let $p \neq 2, 5$ be prime satisfying $p \equiv \pm 1 \mod (5)$ and $p \equiv 3 \mod (4)$. Then $\sigma(p) = \pi(p)$, and therefore divides $p-1$.*

Proof. Since $p \equiv 3 \mod (4)$, we can write $p = 4k+3$ for some k. From Proposition 9 (i) we know that $\pi(p)$ divides $p - 1 = 4k + 2$. if $\sigma(p) \neq \pi(p)$, then $\sigma(p) = \frac{1}{2}\pi(p)$ and must therefore divide $2k+1$. By Proposition 11 this is a contradiction, as $\sigma(p)$ is even for $p \neq 2$. □

For those primes equivalent to 1 or 9 modulo 20 we do not have a complete picture. There are instances of such p with $\theta(p) = 1$ and and instances with $\theta(p) = -1$, in both congruence classes. See the next section for a conjecture in this case.

The primes $p \equiv 1, 9 \mod (20)$ are reducible, so we are still able to derive a total bound on the size of $\sigma(m)$.

Theorem 18. *The Pisano semiperiod satisfies $\sigma(m) \leq 4m$, with equality if and only if $m = 2 \cdot 3 \cdot 5^j$ for some $j > 0$.*

Proof. The bound is easy to establish. We have $\sigma(m) \leq \pi(m) \leq 6m$. But $\pi(m) = 6m$ if and only if $m = 2 \cdot 5^j$, otherwise $\pi(m) \leq 4m$. So either $\sigma(2 \cdot 5^j) = \pi(2 \cdot 5^j)$, or $\sigma(m) \leq 4m$. But by Proposition 13 (iii) we know that $\theta(2 \cdot 5^j) = -1$, so $\sigma(2 \cdot 5^j) = \frac{1}{2}\pi(2 \cdot 5^j)$ and the bound $\sigma(m) \leq 4m$ follows.
As discussed in the proof of Theorem 10, reducible primes can contribute a maximum of $\frac{p-1}{p}$ to $\frac{\sigma(m)}{m}$, so they can once again be safely ignored. If $\theta(m) = -1$, and $m \neq 2$, then $\sigma(m) = \frac{1}{2}m \leq \frac{1}{2}6m = 3m$. So we restrict our attention to products $m = 2^i \cdot 5^j \cdot p_1^{a_1} \cdots p_r^{a_r}$ (i and j may be 0) with p_i irreducible such that $\pi(m) = 4m$ and $\theta(m) = 1$. We use the following facts from the proof of Theorem 10:

(i) If 2 does not divide m, then $\pi(m) = 4m$ is achieved only when $m = 5^j$.
(ii) If 2 does not divide m, and $m \neq 5^j$, then $\pi(m) \leq \frac{8}{3}m$, with equality if and only if $m = 3^k$ or $m = 5^j \cdot 3^k$.
(iii) If 4 divides m, then $\pi(m) \leq 3m$.
(vi) For any m' we have $\pi(2m') \leq 3\pi(m')$, with equality if 3 does not divide $\pi(m')$.

As $\theta(5^j) = -1$, the value $m = 5^j$ does not give $\sigma(m) = 4m$, so by the first fact we can rule out all m such that 2 does not divide m. By the third fact we can rule

out all m with a factor of 4, and consider only those numbers of the form $m = 2m'$ with m' odd. By the fourth fact $\pi(2m') \leq 3\pi(m')$, so $\pi(2m') = 4m$ implies that $\pi(m') \geq \frac{8}{3}m'$. This is achieved only in the cases $m' = 5^j$, $m' = 3^k$ or $m' = 5^j \cdot 3^k$, by the first and second facts. By Proposition 13 (ii) we can rule out the cases $m = 2 \cdot 3^k$ and $m = 2 \cdot 5^j$, as these have $\theta(m) = -1$, so $\sigma(m) = \frac{1}{2}\pi(m) \leq 2m$. Therefore we can only possibly have $\sigma(m) = 4m$ for $m = 2 \cdot 3^k \cdot 5^j$. By Proposition 13 (ii), this has $\theta(m) = 1$, as $\sigma(3^k) = 4 \cdot 3^{k-1}$ and $\sigma(5^j) = 2 \cdot 5^j$ have unequal 2-adic valuations. Finally we calculate:

$$\begin{aligned}
\sigma(m) &= \pi(m) \\
&= \pi(2 \cdot 3^k \cdot 5^j) \\
&= \operatorname{lcm}(\pi(2), \pi(3^k), \pi(5^j)) \\
&= \operatorname{lcm}(3, 8 \cdot 3^{k-1}, 4 \cdot 5^j) \\
&= 8 \cdot 5^j \cdot 3^{\max\{1,k-1\}}
\end{aligned}$$

$$\begin{aligned}
\tfrac{\sigma(m)}{m} &= (8 \cdot 5^j \cdot 3^{\max\{1,k-1\}}) \cdot (2^{-1} \cdot 3^{-k} \cdot 5^{-j}) \\
&= 4 \cdot 3^{\max\{1-k,-1\}}.
\end{aligned}$$

Thus $\sigma(m) = 4m$ is achieved exactly when $k = 1$, i.e., when $m = 2 \cdot 3 \cdot 5^j$. □

3. Unknown cases

As noted above, for primes in the congruence classes 1 and 9 modulo 20 we do not have a good explanation of when the Pisano signature is 1 and when it is -1. There are primes in each class with $\theta(m) = 1$, and primes in each class with $\theta(m) = -1$, Computer experiments indicate that there seem to be more primes with $\theta(m) = -1$ than $\theta(m) = 1$ in both classes.

References

[FB92] Peter Freyd and Kevin S. Brown, *Problems and Solutions: Solutions: E3410*, Amer. Math. Monthly **99** (1992), no. 3, 278–279.

[Rob63] D. W. Robinson, *The Fibonacci matrix modulo m*, Fibonacci Quart **1** (1963), no. 2, 29–36. MR 0158856 (28 #2079)

[SS16] David Singerman and James Strudwick, *Petrie polygons and Farey maps*, To appear in Ars Math. Contemp. (2016).

[Wal60] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly **67** (1960), 525–532.