THEOREM OF THE DAY

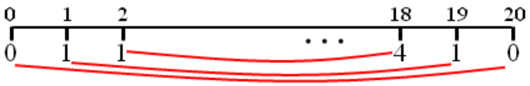
A Theorem on Modular Fibonacci Periodicity *Suppose that $(F_n)_{n\geq 0}$ is the sequence of Fibonacci numbers defined by $F_0 = 0, F_1 = 1$ and, for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Let m be a positive integer and let $(f_n)_{n\geq 0}$ be the Fibonacci sequence taken modulo m, i.e. for $n \geq 0$, let $f_n = F_n \pmod{m}$. Then*

1. *the sequence (f_n) takes the value zero periodically, with period, say, $d(m)$;*
2. *the sequence (f_n) itself is periodic with period, say, $\pi(m)$. Moreover $\pi(m)$ is even when $m > 2$.*

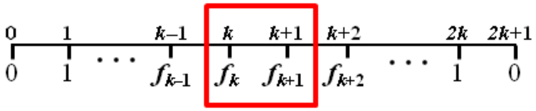
n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946
mod 2	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
mod 4	0	1	1	2	3	1	0	1	1	2	3	1	0	1	1	2	3	1	0	1	1	2
mod 5	0	1	1	2	3	0	3	3	1	4	0	4	4	3	2	0	2	2	4	1	0	1

The values of $F_0, \ldots, F_{21}$ are tabulated above, with reduction by various moduli. We observe that, in the notation of the theorem, $d(2) = \pi(2) = 3$ and $d(4) = \pi(4) = 6$; for $m = 5$, the values of d and π differ: $d(5) = 5, \pi(5) = 20$. We will prove the curious fact that $\pi(m)$ is always even, when $m > 2$. In fact, we will give two proofs: one will reveal *why* the phenomenon occurs; the other will be the proof 'from the book': so delightfully concise and cunning that it gives *nothing* away!

Proof 1 (assumes existence of $d(m)$ and $\pi(m)$)
Observe that, if we pair off entries over a complete period from f_0 to $f_{\pi(m)}$, counting inwards, the paired entries alternately sum to 0 (mod m) (evens), and are equal (odds). E.g. for $m = 5$ we have:



Now suppose $\pi(m)$ is odd, say $\pi(m) = 2k + 1$. Then counting into the middle of the first period we will finish with a middle pair: f_k, f_{k+1}, as shown below.



Now if k is even then $f_k + f_{k+1} = 0 \pmod{m}$. Then $f_{k+2} = 0$ since, by definition, $f_{k+2} = f_k + f_{k+1} \pmod{m}$. But then $f_{k-1} = 0$ because f_{k-1} and f_{k+2} form an odd pairing. And if k is odd then $f_k = f_{k+1}$. But since $f_{k+1} = f_k + f_{k-1}$ this means that $f_{k-1} = 0$. Now f_{k+2} must be 0 because f_{k-1} and f_{k+2} are an even pairing and sum to $0 \pmod{m}$. Either way, we have found a subsequence '$0 \times \times 0$' and we conclude that $d(m) = 1$ or $d(m) = 3$. This means that $F_1 = 1 = 0 \pmod{m}$ or $F_2 = 2 = 0 \pmod{m}$, respectively. Either way, the assumption that $\pi(m)$ is odd has implied that $m \leq 2$.

Proof 2 (assumes existence of $\pi(m)$)
Let $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, the so-called 'Fibonacci matrix'. It is easy to confirm that $Q^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}$. Then $1 = \det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \det\left(Q^{\pi(m)} \pmod{m}\right) = \left(\det Q^{\pi(m)}\right) \pmod{m} = (\det Q)^{\pi(m)} \pmod{m} = (-1)^{\pi(m)} \pmod{m}$, which implies that $\pi(m)$ is even or $m = 1$ or 2.

The periodicity of the 'reduced' Fibonacci sequence was known to Lagrange in the 1780s and its divisibility properties were studied by Edouard Lucas in the 1870s. The modular periodicity of linear recurrences in general was systematically studied by Robert Carmichael in the 1920s and Morgan Ward in the 1930s. This theorem, as stated, is due to Donald Dines Wall (1960) who also gave Proof 1 above. The book proof shown here (Proof 2) is due to David Singerman.

Web link: webspace.ship.edu/msrenault/fibonacci/fib.htm (contains another proof 'from the book' of even periodicity).
Further reading: *The Golden Ratio and Fibonacci Numbers* by R.A Dunlap, World Scientific, 1998.