ALMOST UNIFORM DISTRIBUTION OF THE FIBONACCI SEQUENCE

Eliot Jacobson
Ohio University, Athens, OH 45701
(Submitted August 1987)

Let $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ $(n \geq 2)$ denote the sequence of Fibonacci numbers. For an integer $m > 1$, recall that (F_n) is *uniformly distributed* modulo m if all residues modulo m occur with the same frequency in any period (see [2], [4]). This happens precisely when $m = 5^k$ with $k > 0$, in which case (F_n) has (shortest) period of length $4 \cdot 5^k$, and each residue occurs four times (see [1], [3]). In this paper we study moduli with more complex distributions.

For any r, $0 \leq r < m$, denote by $\nu(r)$ the number of times r occurs as a residue in one (shortest) period of F_n (mod m). If m is a power of 5, then $\nu(r) = 4$ for all r. However, if $m = 11$, then the period of F_n (mod 11) is 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, so that $\nu(r)$ takes on four different values.

Definition: For an integer $m > 1$, (F_n) is *almost uniformly distributed* modulo m [notation: (F_n) AUD (mod m)] if $\nu(r)$ assumes exactly two values for $0 \leq r < m$.

In this paper we describe four infinite sequences of AUD moduli, along with describing the function ν precisely for these moduli. Our proof makes use of a recent result of Velez [2], which we state here for the reader's convenience.

Lemma: For any integer $s \geq 0$, the sequence

$$F_{s+4q},\ q = 0, 1, \ldots, 5^k - 1,$$

consists of a complete residue system modulo 5^k.

Main Theorem: (F_n) is AUD (mod m) for $m \in \{2 \cdot 5^k, 4 \cdot 5^k, 3 \cdot 5^k, 9 \cdot 5^k : k \geq 0\}$. For these moduli, the following data appertain:

Modulus	Period	Distribution
2	3	$\nu(0) = 1, \quad \nu(1) = 2$
4	6	$\nu(0) = \nu(2) = \nu(3) = 1, \ \nu(1) = 3$
$2 \cdot 5^k,\ k > 0$	$3 \cdot 4 \cdot 5^k$	$\nu(r) = \begin{cases} 4 & r \text{ is even} \\ 8 & r \text{ is odd} \end{cases}$
$4 \cdot 5^k,\ k > 0$	$3 \cdot 4 \cdot 5^k$	$\nu(r) = \begin{cases} 2 & r \not\equiv 1 \pmod 4 \\ 6 & r \equiv 1 \pmod 4 \end{cases}$
$3 \cdot 5^k,\ k \geq 0$	$8 \cdot 5^k$	$\nu(r) = \begin{cases} 2 & r \equiv 0 \pmod 3 \\ 3 & r \not\equiv 0 \pmod 3 \end{cases}$
$9 \cdot 5^k,\ k \geq 0$	$3 \cdot 8 \cdot 5^k$	$\nu(r) = \begin{cases} 2 & r \not\equiv 1, 8 \pmod 9 \\ 5 & r \equiv 1, 8 \pmod 9 \end{cases}$

Proof: The cases $m = 2, 3, 4, 9$ can be checked directly. Assume that $k \geq 1$. Because of the similarity of the proofs of the four cases, we only prove the cases $m = 2 \cdot 5^k$ and $m = 9 \cdot 5^k$, leaving the proofs of the remaining cases to the reader.

Case 1. $m = 2 \cdot 5^k$. As the period of $F_n \pmod{m}$ is the least common multiple of its periods modulo 2 and 5^k, it is clear that the period is $3 \cdot 4 \cdot 5^k$.

To compute $\nu(r)$, it suffices, by the Chinese Remainder Theorem, to compute the number of simultaneous solutions to the system

$$\begin{cases} F_n \equiv r_1 \pmod{2} \\ F_n \equiv r_2 \pmod{5^k} \end{cases}$$

with $0 \le n < 3 \cdot 4 \cdot 5^k$, for ordered pairs of residues (r_1, r_2) with $0 \le r_1 < 2$ and $0 \le r_2 < 5^k$. Fix r_2.

For n in the indicated range, n can be expressed uniquely in the form $n = s + 4q$, with $0 \le s < 4$ and $0 \le q \le 3 \cdot 5^k - 1$. By the lemma, for fixed s, there is a unique q_1 with $0 \le q_1 \le 5^k - 1$ such that

$$F_{s+4q_1} \equiv r_2 \pmod{5^k}.$$

Then, also,

$$F_{s+4(q_1+5^k)} \equiv r_2 \pmod{5^k}$$

and

$$F_{s+4(q_1+2\cdot 5^k)} \equiv r_2 \pmod{5^k},$$

because F_n has period $4 \cdot 5^k$ modulo 5^k. Now observe that

$$s + 4q_1 \equiv s + q_1 \pmod{3},$$

$$s + 4(q_1 + 5^k) \equiv s + q_1 + (-1)^k \pmod{3},$$

$$s + 4(q_1 + 2 \cdot 5^k) \equiv s + q_1 + (-1)^{k+1} \pmod{3},$$

and these are incongruent modulo 3. Thus, for fixed s, there are exactly two solutions q to the system

$$\begin{cases} F_{s+4q} \equiv 1 \pmod{2} \\ F_{s+4q} \equiv r_2 \pmod{5^k} \end{cases}$$

and exactly one solution q of the system

$$\begin{cases} F_{s+4q} \equiv 0 \pmod{2} \\ F_{s+4q} \equiv r_2 \pmod{5^k} \end{cases}$$

with $0 \le q \le 3 \cdot 5^k - 1$.

Now s has four possible values, so that there are exactly eight solutions of

$$\begin{cases} F_n \equiv 1 \pmod{2} \\ F_n \equiv r_2 \pmod{5^k} \end{cases}$$

and exactly four solutions of

$$\begin{cases} F_n \equiv 0 \pmod{2} \\ F_n \equiv r_2 \pmod{5^k} \end{cases}$$

with $0 \le n \le 3 \cdot 4 \cdot 5^k - 1$. This translates via the Chinese Remainder Theorem to the stated distribution.

The method of proof is now clear, and we provide few details in Case 2.

Case 2. $m = 9 \cdot 5^k$. The period is $\operatorname{lcm}(24, 4 \cdot 5^k) = 8 \cdot 3 \cdot 5^k$. Express $n = s + 4q$, where $0 \le s \le 3$, $0 \le q \le 6 \cdot 5^k - 1$. For fixed s and residue $r_2 \pmod{5^k}$, there is a unique q_1 such that $F_{s+4q_1} \equiv r_2 \pmod{5^k}$ with $0 \le q_1 \le 5^k - 1$. Now the Fibonacci numbers have period 0, 1, 1, 2, 3, 5, 8, 4, 3, 7, 1, 8, 0, 8, 8, 7, 6, 4, 1, 5, 6, 2, 8, 1 (mod 9) of length 24, so we consider the subscripts $s + 4(q_1 + t \cdot 5^k) \pmod{24}$ for $t = 0, 1, 2, 3, 4, 5$. A straightforward calculation yields that these are congruent (in some order) to s, $s + 4$, $s + 8$, $s + 12$, $s + 16$, $s + 20$ (mod 24). Thus, for fixed s, r_2 there are 6 values of q, $0 \le q \le 6 \cdot 5^k - 1$, with $F_{s+4q} \equiv r_2 \pmod{5^k}$, (namely, $q = q_1 + t \cdot 5^k$, $0 \le t \le 5$). Now, for this sequence of q's, we have that:

$$\underline{s = 0} \Rightarrow F_{s+4q} \equiv 0, 3, 3, 0, 6, 6 \pmod 9$$
$$\underline{s = 1} \Rightarrow F_{s+4q} \equiv 1, 5, 7, 8, 4, 2 \pmod 9$$
$$\underline{s = 2} \Rightarrow F_{s+4q} \equiv 1, 8, 1, 8, 1, 8 \pmod 9$$
$$\underline{s = 3} \Rightarrow F_{s+4q} \equiv 2, 4, 8, 7, 5, 1 \pmod 9$$

Again, the stated distribution follows from the Chinese Remainder Theorem. □

Remarks: It is clear from the proof that the given method will decide the distribution of any family of the form $m \cdot 5^k$, where $5 \nmid m$, once it is known explicitly modulo m. However, there does not appear to be a general theorem valid for all m that will let one forgo this tedium.

It is natural to ask if the list in the Theorem is complete. A computer search of moduli $m \le 1000$ indicates this is so. However, the converse proof quickly reduces to showing that a modulus m where ν takes on only the values 0 and f for that m does not exist. The question of whether there exists a prime $p > 7$ such that only the frequencies 0 and f occur mod p is a well-known open problem.

References

1. R. T. Bumby. "A Distribution Property for Linear Recurrence of the Second Order." *Proc. Amer. Math. Soc.* *50* (1975):101-106.
2. L. Kuipers & H. Niederreiter. *Uniform Distribution of Sequences.* New York: Wiley-Interscience, 1974.
3. W. Narkiewicz. "Uniform Distribution of Sequences of Integers in Residue Classes." In *Lecture Notes in Mathematics*, Vol. 1087. New York: Springer-Verlag, 1984.
4. I. Niven. "Uniform Distribution of Sequences of Integers." *Trans. Amer. Math. Soc.* *98* (1961):52-61.
5. W. Y. Velez. "Uniform Distribution of Two-Term Recurrence Sequences." *Trans. Amer. Math. Soc.* *301* (1987):37-45.

*****