DISTRIBUTION OF THE FIBONACCI NUMBERS MOD 2^K

Eliot T. Jacobson
Ohio University, Athens, OH 45701
(Submitted September 1990)

Let $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$, denote the sequence of Fibonacci Numbers. For any modulus $m \geq 2$, and residue $b \pmod{m}$, denote by $v(m, b)$ the number of occurrences of b as a residue in one (shortest) period of $F_n \pmod{m}$.

If $m = 5$ with $k > 0$, then $F_n \pmod{5^k}$ has shortest period of length $4 \cdot 5^k$, and $v(5^k, b) = 4$ for all $b \pmod{5^k}$. This is so-called *uniform distribution*, and has been studied in great detail by a number of authors (e.g., [1], [4], [5], [6]). However, the study of the function $v(m, b)$ for moduli other than 5 is still relatively unexplored. Some recent work in this area can be found in [2] and [3].

In this paper we completely describe the function $v(m, b)$ when $m = 2^k$, $k \geq 1$. What makes this possible is a type of stability that occurs when $k \geq 5$. This stability does not seem to appear for primes other than $p = 2, 5$ (which somehow is not surprising). Of course, the values of $v(2^k, b)$ for $k = 1, 2, 3, 4$ are easily checked by hand. We include these values for completeness.

Main Theorem

For $F_n \pmod{2^k}$, with $k \geq 1$, the following data appertain:

For $1 \leq k \leq 4$:

$v(2, 0) = 1$,
$v(2, 1) = 2$,
$v(4, 0) = v(4, 2) = 1$,
$v(8, 0) = v(8, 2) = v(16, 0) = v(16, 8) = 2$,
$v(16, 2) = 4$,
$v(2^k, b) = 1$ if $b \equiv 3 \pmod{4}$ and $2 \leq k \leq 4$,
$v(2^k, b) = 3$ if $b \equiv 1 \pmod{4}$ and $2 \leq k \leq 4$, and
$v(2^k, b) = 0$ in all other cases, $1 \leq k \leq 4$.

For $k \geq 5$:

$$v(2^k, b) = \begin{cases} 1, & \text{if } b \equiv 3 \pmod{4}, \\ 2, & \text{if } b \equiv 0 \pmod{8}, \\ 3, & \text{if } b \equiv 1 \pmod{4}, \\ 8, & \text{if } b \equiv 2 \pmod{32}, \\ 0, & \text{for all other residues.} \end{cases}$$

Most of our proofs proceed either by induction, or by invoking a standard formula for the Fibonacci sequence. Perhaps there are other proofs of our Theorem, but because of the absence in the literature of a convenient closed form for $F_n \pmod{2^k}$, our methodology is quite computational. Because of their frequent use, we record the following two standard formulas.

<u>Addition Formula</u>: If $m \geq 1$ and $n \geq 0$, then

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

<u>Subtraction Forumla</u>: If $m \geq n > 0$, then

$$F_{m-n} = (-1)^{n+1} \cdot (F_{m-1}F_n - F_mF_{n-1}).$$

The main body of this paper consists in establishing a number of congruences for $F_n \pmod{2^k}$.

Lemma 1: Let $k \geq 5$. Then

$$\begin{aligned} F_{2^{k-3}\cdot 3-1} &\equiv 1 - 2^{k-2} \pmod{2^k}, \\ F_{2^{k-3}\cdot 3} &\equiv 2^{k-1} \pmod{2^{k+1}} \end{aligned}$$

Proof: We prove these formulas simultaneously by induction on k. When $k = 5$, the results are easily checked. Now assume the result is true for $k \geq 5$, and write

$$\begin{aligned} F_{2^{k-3}\cdot 3-1} &= 1 - 2^{k-2}u \\ F_{2^{k-3}\cdot 3} &= 2^{k-1}v \end{aligned}$$

where $u, v \equiv 1 \pmod 4$. Note that as $k \geq 5$, we have $(k - 2) + (k - 2) \geq k + 1$, and $(k - 2) + (k - 1) \geq k + 2$. Thus,

$$\begin{aligned} F_{2^{k-2}\cdot 3-1} &= F_{2^{k-3}\cdot 3-1+2^{k-3}\cdot 3} \\ &= F_{2^{k-3}\cdot 3-2}F_{2^{k-3}\cdot 3} + F_{2^{k-3}\cdot 3-1}F_{2^{k-3}\cdot 3+1} \\ &= (2^{k-1}v - 1 + 2^{k-2}u)2^{k-1}v + (1 - 2^{k-2}u)(2^{k-1}v + 1 - 2^{k-2}u) \\ &\equiv -2^{k-1}v + 2^{k-1}v + 1 - 2^{k-2}u - 2^{k-2}u \pmod{2^{k+1}} \\ &\equiv 1 - 2^{k-1} \pmod{2^{k+1}} \end{aligned}$$

and

$$\begin{aligned} F_{2^{k-2}\cdot 3} &= F_{2^{k-3}\cdot 3+2^{k-3}\cdot 3} \\ &= (1 - 2^{k-2}u)2^{k-1}v + 2^{k-1}v(2^{k-1}v + 1 - 2^{k-2}u) \\ &\equiv 2^{k-1}v + 2^{k-1}v \pmod{2^{k+2}} \\ &\equiv 2^k \pmod{2^{k+2}}. \end{aligned}$$

One consequence of this lemma is that $F_n \pmod{2^k}$ has shortest period of length $2^{k-1}\cdot 3$.

Lemma 2: Let $k \geq 5$ and $s \geq 1$. Then,

$$\begin{aligned} F_{2^{k-3}\cdot 3s-1} &\equiv 1 - s\cdot 2^{k-2} \pmod{2^k}, \text{ and} \\ F_{2^{k-3}\cdot 3s} &\equiv s\cdot 2^{k-1} \pmod{2^k}. \end{aligned}$$

Proof: Lemma 1 is the case $s = 1$. Now proceed by induction on s, by applying the addition formula and Lemma 1 to

$$\begin{aligned} F_{2^{k-3}\cdot 3s-1} &= F_{2^{k-3}\cdot 3(s-1)-1+2^{k-3}\cdot 3} \text{ and} \\ F_{2^{k-3}\cdot 3s} &= F_{2^{k-3}\cdot 3(s-1)+2^{k-3}\cdot 3}. \end{aligned}$$

The details are omitted.

Lemma 3: Let $k \geq 5$ and $n \geq 0$. Then,

$$F_{n+2^{k-2}\cdot 3} \equiv \begin{cases} F_n \pmod{2^k} & \text{if } n \equiv 0 \pmod 3, \\ F_n + 2^{k-1} \pmod{2^k} & \text{if } n \equiv 1,\ 2 \pmod 3. \end{cases}$$

Proof: By Lemma 1,

$$F_{2^{k-2}\cdot 3} \equiv 0 \pmod{2^k} \quad \text{and} \quad F_{2^{k-2}\cdot 3-1} \equiv 1 - 2^{k-1} \pmod{2^k}.$$

Thus,

$$\begin{aligned} F_{n+2^{k-2}\cdot 3} &= F_{n-1}F_{2^{k-2}\cdot 3} + F_n(F_{2^{k-2}\cdot 3} + F_{2^{k-2}\cdot 3-1}) \\ &\equiv F_nF_{2^{k-2}\cdot 3-1} \pmod{2^k} \equiv F_n(1 - 2^{k-1}) \pmod{2^k}. \end{aligned}$$

The result follows since F_n is even precisely when $n \equiv 0 \pmod 3$.

In our subsequent work we will frequently have need of the residues of F_n (mod 4) and F_n (mod 6). We record one period of each here, from which the reader can deduce the requisite congruences:

F_n (mod 4): 0, 1, 1, 2, 3, 1
F_n (mod 6): 0, 1, 1, 2, 3, 5, 2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1

Lemma 4: Let $k \geq 5$ and $n \geq 0$ and assume $n \equiv 0 \pmod 6$. Then,

$$F_{n+2^{k-3}\cdot 3} \equiv F_n + 2^{k-1} \pmod{2^k}.$$

Proof: Analogous to the previous proof. Note that $n \equiv 0 \pmod 6$ if and only if $F_n \equiv 0 \pmod 4$.

Lemma 5: If $n \equiv 3 \pmod 6$, then $F_n \equiv 2 \pmod{32}$.

Proof: Write $n = 6t + 3$ with $t \geq 0$; use induction on t together with an application of the addition formula to $F_{6(t+1)+3} = F_{6(t+3)+6}$.

Lemma 6: If $n \equiv 3 \pmod 6$ and $k \geq 5$, then for all $s \geq 1$,

$$F_{2^{k-3}\cdot 3s \pm n} \equiv F_n \pmod{2^k}.$$

Proof: We treat the two cases ± separately.

Case +:

$$\begin{aligned} F_{2^{k-3}\cdot 3s+n} &= F_{2^{k-3}\cdot 3s-1}F_n + F_{2^{k-3}\cdot 3s}F_{n+1} \\ &\equiv (1 - s\cdot 2^{k-2})F_n + s\cdot 2^{k-1} \pmod{2^k} \\ &\equiv F_n - s\cdot 2^{k-1} + s\cdot 2^{k-1} \pmod{2^k} \\ &\equiv F_n \pmod{2^k}. \end{aligned}$$

Case −: Of course, we are tacitly assuming $2^{k-3}\cdot 3s - n > 0$. We use the subtraction formula

$$\begin{aligned} F_{2^{k-3}\cdot 3s-n} &= (-1)^{n+1}\cdot(F_{2^{k-3}\cdot 3s-1}F_n - F_{2^{k-3}\cdot 3s}F_{n-1}) \\ &\equiv (1 - s\cdot 2^{k-2})F_n - s\cdot 2^{k-1}F_{n-1} \pmod{2^k} \\ &\equiv F_n - s\cdot 2^{k-1} - s\cdot 2^{k-1} \pmod{2^k} \\ &\equiv F_n \pmod{2^k}. \end{aligned}$$

Lemma 7: If $n \equiv 3 \pmod 6$ and $k \geq 6$, then,

$$F_{n+2^{k-4}\cdot 3} \equiv F_n + 2^{k-1} \pmod{2^k}.$$

Proof: By Lemma 1, write

$$F_{2^{k-4}\cdot 3} = 2^{k-2}\cdot u \quad\text{and}\quad F_{2^{k-4}\cdot 3-1} = 1 - 2^{k-3}\cdot v,$$

where $u, v \equiv 1 \pmod 4$. Then, by the addition formula and Lemma 5,

$$\begin{aligned} F_{n+2^{k-4}\cdot 3} &= F_{n-1}\cdot 2^{k-2}u + F_n(2^{k-2}u + 1 - 2^{k-3}v) \\ &\equiv 2^{k-2}u + 2^{k-1}u + F_n - 2^{k-2}v \pmod{2^k} \\ &\equiv 2^{k-2} + 2^{k-1} + F_n - 2^{k-2} \pmod{2^k} \\ &\equiv 2^{k-1} + F_n \pmod{2^k}. \end{aligned}$$

Proof of the Main Theorem

We proceed by induction on $k \geq 5$. The result is easily checked for $k = 5$, so assume $k \geq 5$ and the Theorem holds for k.

First, if $b \equiv 4, 6, 10, 12, 14, 18, 20, 22, 26, 28, 30 \pmod{32}$, then it is clear that $v(2^{k+1}, b) = 0$ since $v(2^5, b) = 0$.

Case 1: $b \equiv 3 \pmod 4$. Then $v(2^k, b) = 1$, so choose n such that $F_n \equiv b \pmod{2^k}$. Since b is odd, we have $n \equiv 1, 2 \pmod 3$. Now either $F_n \equiv b \pmod{2^{k+1}}$ or $F_n \equiv b + 2^k \pmod{2^{k+1}}$. In the latter case, Lemma 3 gives

$$\begin{aligned} F_{n+2^{k-1}\cdot 3} &\equiv F_n + 2^k \pmod{2^{k+1}} \equiv b + 2^k + 2^k \pmod{2^{k+1}} \\ &\equiv b \pmod{2^{k+1}}. \end{aligned}$$

Therefore, $v(2^{k+1}, b) \geq 1$ when $b \equiv 3 \pmod 4$.

Case 2: $b \equiv 1 \pmod 4$. Then $(2^k, b) = 3$, so choose

$$0 < n_1 < n_2 < n_3 < 2^{k-1}\cdot 3,$$

with $F_{n_i} \equiv b$ (mod 2) for all i. Then, as above, for each i, either

$$F_{n_i} \equiv b \pmod{2^{k+1}} \quad \text{or} \quad F_{n_i+2^{k-1}\cdot 3} \equiv b \pmod{2^{k+1}}.$$

So, $v(2^{k+1}, b) \geq 3$ when $b \equiv 1 \pmod 4$.

Case 3: $b \equiv 0 \pmod 8$. Then $v(2^k, b) = 2$, so let

$$0 < m < n < 2^{k-1}\cdot 3$$

be such that $F_m \equiv F_n \equiv b \pmod{2^k}$. Note that as $F_m \equiv F_n \equiv 0 \pmod 4$, we have $m \equiv n \equiv 0 \pmod 6$, so Lemma 4 applies. In particular,

$$F_{m+2^{k-2}\cdot 3} \equiv F_m \pmod{2^k},$$

from which it follows that $m < 2^{k-2}\cdot 3$ and $n = m + 2^{k-2}\cdot 3$.

If $F_m \equiv b \pmod{2^{k+1}}$, then by Lemma 3,

$$F_{m+2^{k-1}\cdot 3} \equiv b \pmod{2^{k+1}},$$

so $v(2^{k+1}, b) \geq 2$. Otherwise, we must have

$$F_m \equiv b + 2^k \pmod{2^{k+1}}.$$

But then by Lemma 4,

$$F_n = F_{m+2^{k-2}\cdot 3} \equiv F_m + 2^k \pmod{2^{k+1}} \equiv b \pmod{2^{k+1}},$$

and also,

$$F_{n+2^{k-1}\cdot 3} \equiv F_n \equiv b \pmod{2^{k+1}}.$$

We conclude that $v(2^{k+1}, b) \geq 2$ when $b \equiv 0 \pmod 8$.

Case 4: $b \equiv 2 \pmod{32}$. Assume that $v(2^k, b) = 8$. Let $F_n \equiv b \pmod{2^k}$, with $n < 2^{k-1}\cdot 3$. Then $F_n \equiv 2 \pmod 4$, so that $n \equiv 3 \pmod 6$. Now either

$$F_n \equiv b \pmod{2^{k+1}} \quad \text{or} \quad F_n \equiv b + 2^k \pmod{2^{k+1}}.$$

In the latter case, by Lemma 7 we have

$$F_{n+2^{k-3}\cdot 3} \equiv F_n + 2^k \equiv b \pmod{2^{k+1}}.$$

Thus, there is at least one index $0 < m < 2^k\cdot 3$ such that $F_m \equiv b \pmod{2^{k+1}}$. But now, by Lemma 6,

$$F_{2^{k-2}\cdot 3s\pm m} \equiv F_m \equiv b \pmod{2^{k+1}} \text{ for } s = 4, 5, 6, 7.$$

Since these eight solutions all occur in one period of $F_n \pmod{2^{k+1}}$, we conclude that $v(2^{k+1}, b) \geq 8$.

Conclusion: We have established inequalities in each case of the Theorem. The proof follows from a straightforward computation, using the fact that F_n has shortest period of length $2^k\cdot 3$ modulo 2^{k+1}, and the obvious identity:

$$\sum_{b \pmod{2^{k+1}}} v(2^{k+1}, b) = 2^k \cdot 3.$$

Using the main Theorem of [2], we are now able to describe the distribution of $F_n \pmod{2^k \cdot 5^j}$. Indeed,

Theorem: For $F_n \pmod{2^k \cdot 5^j}$ with $k \geq 5$ and $j \geq 0$, we have

$$v(2^k \cdot 5^j, b) = \begin{cases} 1, & \text{if } b \equiv 3 \pmod 4, \\ 2, & \text{if } b \equiv 0 \pmod 8, \\ 3, & \text{if } b \equiv 1 \pmod 4, \\ 8, & \text{if } b \equiv 2 \pmod{32}, \\ 0, & \text{for all other residues.} \end{cases}$$

References

1. R. T. Bumby. "A Distribution Property for Linear Recurrence of the Second Order." *Proc. Amer. Math. Soc.* *50* (1975):101-06.
2. E. T. Jacobson. "The Distribution of Residues of Two-Term Recurrence Sequences." *Fibonacci Quarterly* *28.3* (1990):227-29.
3. E. T. Jacobson. "A Brief Survey on Distribution Questions for Second Order Linear Recurrences." *Proceedings of the First Meeting of the Canadian Number Theory Association.* Ed. Richard A. Mollin. Walter de Bruyter, 1990, pp. 249-54.
4. L. Kuipers & J. Shiue. "A Distribution Property of the Sequence of Fibonacci Numbers." *Fibonacci Quarterly* *10.5* (1972):375-76, 392.
5. H. Niederreiter. "Distribution of Fibonacci Numbers Mod 5^K." *Fibonacci Quarterly* *10.5* (1972):373-74.
6. W. Y. Velez. "Uniform Distribution of Two-Term Recurrence Sequences." *Trans. Amer. Math. Soc.* *301* (1987):37-45.

AMS Classification numbers: 11B50, 11K36.

*****