CERTAIN CONGRUENCE PROPERTIES (MODULO 100) OF FIBONACCI NUMBERS

MICHAEL R. TURNER
Regis College, Denver, Colorado 80221

Remark. It was originally observed by the author that if p is a prime ≥ 5, then $F_{p^2} \equiv p^2 \pmod{100}$. Further study led to this theorem which characterizes those Fibonacci numbers which terminate in the same last two digits as their indices. The original observation is proved as a corollary to the theorem.

Theorem. $F_n \equiv n \pmod{100}$ if and only if

$$n \equiv 1,\ 5,\ 25,\ 29,\ 41, \text{ or } 49 \pmod{60} \text{ or } n \equiv 0 \pmod{300}.$$

Proof. From [1], we have the well known formula

$$(1) \qquad F_n = 2^{1-n}\left[\binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \cdots + 5^{\frac{m-1}{2}}\binom{n}{m}\right],$$

where $m = n$ if n is odd, and $m = n - 1$ if n is even.

Lemma 1. $F_{60k} \equiv 20k \pmod{100}$.

Proof. Observe that (1) implies

$$(2) \qquad 2^{n-1}F_n \equiv n + 5\,\frac{n(n-1)(n-2)}{6} \pmod{25}.$$

From [1], we have for $n, m \geq 2$, $(n,m) = d$ implies that $(F_n, F_m) = F_d$. Now (2) implies $2^{60k-1}F_{60k} \equiv 60k + 50k(60k-1)(60k-2) \pmod{25}$, which reduces to $2^{60k-1}F_{60k} \equiv 10k \pmod{25}$. Since $2^{20} \equiv 1 \pmod{25}$, we get $F_{60k} \equiv 20k \pmod{25}$. Since 6 divides $60k$, it follows that F_6 divides F_{60k}. Now $F_6 = 8$, so $F_{60k} \equiv 0 \pmod 4$. Combining this with $F_{60k} \equiv 20k \pmod{25}$, we get $F_{60k} \equiv 20k \pmod{100}$, which proves Lemma 1.

We now prove one of the congruences in the theorem.

$$(3) \qquad n \equiv 1 \pmod{60} \text{ implies } F_n \equiv n \pmod{100}.$$

Proof. Clearly $n = 1$ implies $F_n \equiv n \pmod{100}$. Assume that for all $k < N$, $n = 60k + 1$ implies $F_n \equiv n \pmod{100}$. Now if $n = 60N + 1$ for even N, then $n = 120k + 1$ for $k = N/2 < N$.

From [2], we have the following identity, which will prove extremely useful in what follows.

$$(4) \qquad F_{n+m+1} = F_nF_m + F_{n+1}F_{m+1}.$$

In particular,

$$F_{120k+1} = F^2_{60k} + F^2_{60k+1} .$$

Using Lemma 1 and induction hypotheses, we get

$$F_n = F^2_{60k+1} + F^2_{60k} \equiv (60k + 1)^2 + (20k)^2 \equiv 120k + 1 = n \pmod{100} .$$

If $n = 60N + 1$ for odd N, then $n = 120k + 60 + 1$ for $k = (N - 1)/2$. Then $F_n = F_{120k}F_{60} + F_{120k+1}F_{61}$. Inspection of any large table such as [3] verifies that $F_{61} \equiv 61 \pmod{100}$. Thus, by Lemma 1 and induction hypothesis, we have

$$F_n \equiv 40k\cdot 20 + (120k + 1)\cdot 61 \equiv 120k + 60 + 1 \equiv n \pmod{100} .$$

This proves the congruence.

Lemma 2. $F_{60k+n} \equiv 20k\cdot F_{n-1} + (60k + 1)\cdot F_n \pmod{100}$.

Proof. Lemma 2 follows from (3) and Lemma 1. The remainder of the proof is divided into five cases.

Case 1. $n \equiv 1 \pmod 5$.

Assume $F_n \equiv n \pmod{100}$. Then $F_n \equiv n \pmod 4$ and $F_n \equiv n \pmod{25}$. Now (2) implies $2^{n-1}F_n \equiv n \pmod{25}$, since

$$5\,\frac{n(n - 1)(n - 2)}{6} \equiv 0 \pmod{25} .$$

Also, $(5,n) = 1$ and $F_n \equiv n \pmod{100}$, so we may cancel the n and F_n to get $2^{n-1} \equiv 1 \pmod{25}$. Since 2 belongs to the exponent 20 (mod 25), it follows that $n \equiv 1 \pmod{20}$. Thus $n \equiv 1 \pmod 4$. But $F_n \equiv n \equiv 1 \pmod 4$, so F_n must be odd. But F_n is even if and only if $n \equiv 0 \pmod 3$, so $n \equiv 1$ or $2 \pmod 3$. Combining results,

$$\left.\begin{matrix} n \equiv 1 \pmod 3 \\ n \equiv 1 \pmod{20} \end{matrix}\right\} n \equiv 1 \pmod{60} \quad \text{or} \quad \left.\begin{matrix} n \equiv 2 \pmod 3 \\ n \equiv 1 \pmod{20} \end{matrix}\right\} n \equiv 41 \pmod{60} .$$

Now suppose that $n \equiv 41 \pmod{60}$. Let $n = 60k + 41$. By Lemma 2,

$$F_n \equiv 20k\cdot F_{40} + (60k + 1)F_{41} \pmod{100} .$$

By inspection of tables, we have $F_{40} \equiv 55 \pmod{100}$ and $F_{41} \equiv 41 \pmod{100}$. Therefore, we have

$$F_n \equiv (60k + 41) + 20k\cdot 55 \equiv 60k + 41 \equiv n \pmod{100} .$$

This result, along with (3), completes the proof of Case 1.

Case 2. $n \equiv 2 \pmod 5$.

This case is impossible, for as in Case 1, it follows that $n \equiv 1 \pmod{20}$, a contradiction.

Case 3. $n \equiv 3 \pmod 5$.

Let $n = 3 + 5k$. Then from (2),

$$2^{2+5k}F_n \equiv n + n \cdot \frac{5(2+5k)(1+5k)}{6} \pmod{25}.$$

Assuming $F_n \equiv n \pmod{100}$, we may cancel the F_n and n's, since $(n,25) = 1$, obtaining $3 \cdot 2^{3+5k} \equiv 6 + 5 \cdot 2 \cdot 1 \pmod{25}$. Thus $2^{5k+6} \equiv 1 \pmod{25}$. But this congruence implies $5k + 6 \equiv 0 \pmod{20}$, or $5k \equiv 14 \pmod{20}$. This congruence is not possible, so case 3 is impossible.

Case 4. $n \equiv 4 \pmod 5$.

Assume $F_n \equiv n \pmod{100}$. Let $n = 4 + 5k$. Then $3 \cdot 2^{4+5k} \equiv 6 + 5 \cdot 3 \cdot 2 \pmod{25}$, so $2^{5k-5} \equiv 1 \pmod{25}$, and $5k \equiv 5 \pmod{20}$. Thus $n = 5k + 4 \equiv 9 \pmod{20}$. F_n and n are therefore odd, so $n \equiv 1$ or $2 \pmod 3$. Combining results,

$$\left.\begin{array}{l} n \equiv 1 \pmod 3 \\ n \equiv 9 \pmod{20} \end{array}\right\} n \equiv 49 \pmod{60} \quad \text{or} \quad \left.\begin{array}{l} n \equiv 2 \pmod 3 \\ n \equiv 9 \pmod{20} \end{array}\right\} n \equiv 29 \pmod{60}.$$

Now suppose that $n \equiv 29 \pmod{60}$. Let $n = 29 + 60k$. By Lemma 2,

$$F_n \equiv F_{60k}F_{28} + F_{60k+1}F_{29} \pmod{100}.$$

By inspection of tables, $F_{28} \equiv 11 \pmod{100}$, and $F_{29} \equiv 29 \pmod{100}$. Thus by Lemma 1, we have

$$F_n \equiv 20k \cdot 11 + (60k + 1) \cdot 29 \equiv 60k + 29 \equiv n \pmod{100}.$$

Suppose $n \equiv 49 \pmod{60}$. Let $n = 49 + 60k$. By similar reasoning,

$$F_n \equiv 20k \cdot F_{48} + (60k + 1)F_{49} \equiv 20k \cdot 76 + (60k + 1) \cdot 49 \equiv 60k + 49 \equiv n \pmod{100}.$$

This result completes the proof of Case 4.

Case 5. $n \equiv 0 \pmod 5$.

Let $n = 5^s \cdot k$, where $s \geq 1$, and $(5,k) = 1$. We shall consider in order the possibilities $n \equiv 0, 1, 2$, and $3 \pmod 4$. Assume $F_n \equiv n \pmod{100}$. If $n \equiv 0 \pmod 4$, and $s = 1$, then $n = 5k$, where $(5,k) = 1$. Thus we get $2^{n-1}F_n \equiv n \pmod{25}$ from (2). Now $F_n \equiv n \equiv 5k \pmod{25}$ implies $2^{n-1} \cdot 5 \equiv 5 \pmod{25}$, so $n \equiv 1 \pmod 4$. But in this case, the last result is impossible, so it follows that $s \geq 2$. Also, since F_n must be even, we have $n \equiv 0 \pmod 3$. Finally, $n \equiv 0 \pmod{5^s}$ implies $n \equiv 0 \pmod{25}$. Combining, we have

$$\left.\begin{array}{l} n \equiv 0 \pmod{3} \\ n \equiv 0 \pmod{4} \\ n \equiv 0 \pmod{25} \end{array}\right\} n \equiv 0 \pmod{300} .$$

Let us suppose that $n \equiv 0 \pmod{4}$; we have F_n odd, so there are two combinations:

$$\left.\begin{array}{l} n \equiv 1 \pmod{3} \\ n \equiv 1 \pmod{4} \\ n \equiv 0 \pmod{5} \end{array}\right\} n \equiv 25 \pmod{60} \quad \text{or} \quad \left.\begin{array}{l} n \equiv 2 \pmod{3} \\ n \equiv 1 \pmod{4} \\ n \equiv 0 \pmod{5} \end{array}\right\} n \equiv 5 \pmod{60} .$$

If $n \equiv 2 \pmod{4}$, we have

$$\left.\begin{array}{l} n \equiv 0 \pmod{3} \\ n \equiv 2 \pmod{4} \\ n \equiv 0 \pmod{5} \end{array}\right\} n \equiv 30 \pmod{60} .$$

Let $n = 30 + 60k$. By Lemmas 1 and 2,

$$F_n = F_{60k+30} \equiv 20kF_{29} + (60k + 1)F_{30} \pmod{100} .$$

But this reduces to $F_n \equiv 20k + 40 \pmod{100}$. Now $F_n \equiv n = 30 + 60k \pmod{100}$ implies $20k + 40 \equiv 60k + 30 \pmod{100}$, or $40k \equiv 10 \pmod{100}$, which is impossible. If $n \equiv 3 \pmod{4}$, we get two combinations:

$$\left.\begin{array}{l} n \equiv 1 \pmod{3} \\ n \equiv 3 \pmod{4} \\ n \equiv 0 \pmod{5} \end{array}\right\} n \equiv 55 \pmod{60} \quad \text{or} \quad \left.\begin{array}{l} n \equiv 2 \pmod{3} \\ n \equiv 3 \pmod{4} \\ n \equiv 0 \pmod{5} \end{array}\right\} n \equiv 35 \pmod{60} .$$

The first congruence results in

$$F_n = F_{55+60k} \equiv 40k + 45 \pmod{100} ,$$

and $F_n \equiv n = 55 + 60k$ implies $20k \equiv 90 \pmod{100}$, which is impossible. The second congruence results in

$$F_n = F_{35+60k} \equiv 40k + 65 \pmod{100} ,$$

and $F_n \equiv n = 35 + 60k$ implies $20k \equiv 30 \pmod{100}$, which is also impossible.

Suppose $n \equiv 5 \pmod{60}$. Let $n = 5 + 60k$. Then $F_n = F_{5+60k}$, so

$$F_n \equiv 20k \cdot F_4 + (60k + 1) \cdot F_5 \equiv 60k + 5 \equiv n \pmod{100} .$$

Suppose $n \equiv 25 \pmod{60}$. Let $n = 25 + 60k$. Then

$$F_n = F_{25} + 60k,$$

so

$$F_n \equiv 20k \cdot F_{24} + (60k + 1) \cdot F_{25} \equiv 60k + 25 \equiv n \pmod{100}.$$

Finally, if $n \equiv 0 \pmod{300}$, then 300 divides n, so F_{300} divides F_n. By Lemma 1, $F_{300} \equiv 0 \pmod{100}$, and thus $F_n \equiv 0 \equiv n \pmod{100}$.

This result completes the proof of the theorem.

Corollary. If p is a prime ≥ 5, then $F_{p^2} \equiv p^2 \pmod{100}$.

Proof. By the theorem, $F_5 \equiv 5 \pmod{100}$. If p is a prime > 5, then

$$p \equiv 1, 3, 7, 9, 11, 13, 17, \text{ or } 19 \pmod{20}.$$

Thus $p^2 \equiv 1$ or $9 \pmod{20}$. Since $p^2 \equiv 1 \pmod 3$, it follows that $p^2 \equiv 1$ or $49 \pmod{60}$.

REFERENCES

1. G. H. Hardy and E. H. Wright, An Introduction to the Theory of Numbers,

2. S. L. Basin and V. E. Hoggatt, Jr., "A Primer on the Fibonacci Sequence, Part I," Fibonacci Quarterly, Vol. 1, No. 1 (Feb. 1963), pp. 65-72.
3. Dov Jarden, Recurring Sequences, Riveon Lematematika, Jerusalem, Israel, 1958.