SOME CONGRUENCES FOR FIBONACCI NUMBERS

A. G. SHANNON
The New South Wales Institute of Technology, Sydney, Australia
and
A. F. HORADAM
University of New England, Armidale, Australia
and
Science Institute, University of Iceland, Reykjavik, Iceland
and
S. N. COLLINGS
The Open University, Bletchley, England

1. INTRODUCTION

The first congruence in this paper arose in an effort to extend a result of Collings [1] and the second congruence is merely an elaboration of part of a theorem of Wall [5]. In the final section we look at some congruences modulo m^2.

Some of the symbols involved are: $D(m)$, the period of divisibility modulo m (or rank of apparition of m or entry point of m), the smallest positive integer z such that $F_z \equiv 0 \pmod m$ (see Daykin and Dresel [2]); $C(m)$, the period of cycle modulo m, the smallest positive integer k: $F_{k+n} \equiv F_n \pmod m$, $n \geqslant 0$; $T(m)$, the smallest positive integer ℓ: $F_{z+1}^{\ell} \equiv 1. \pmod m$. In fact, $z\ell = k$. (See Wyler [6].)

Collings' result was than when m is prime, ℓ is even,

(1.1) $$F_r + F_{\frac{1}{2}\ell z+r} \equiv 0 \pmod m,$$

where

$$F_n = F_{n-1} + F_{n-2} \quad (n \geqslant 3), \qquad F_1 = F_2 = 1\,.$$

We show that m can be composite if $F_{z+1}^{\frac{1}{2}\ell} \equiv -1 \pmod m$.

2. LEMMAS

Lemma 2.1: (see Vinson [5].)

For $m > 2$, $D(m)$ is odd implies that $T(m) = 4$; and $D(m)$ is even implies that $T(m) = 1$ or 2.

Proof: Simson's relation can be expressed as

$$\begin{aligned} F_{z+1}^2 &= F_{z+2}F_z + (-1)^{z+2} \\ &\equiv (-1)^{z+2} \quad \text{since} \quad F_z \equiv 0 \pmod m, \\ &\equiv 1 \pmod m \quad \text{if} \quad z = D(m) \quad \text{is even,} \\ &\equiv -1 \pmod m \quad \text{if} \quad z = D(m) \quad \text{is odd.} \end{aligned}$$

When

$$\begin{aligned} F_{z+1}^2 &\equiv 1 \pmod m, \\ T(m) &= 2 \quad \text{if} \quad F_{z+1} \not\equiv 1 \pmod m, \\ T(m) &= 1 \quad \text{if} \quad F_{z+1} \equiv 1 \pmod m. \end{aligned}$$

When

$$\begin{aligned} F_{z+1}^2 &\equiv -1 \pmod m, \\ F_{z+1}^2 &\equiv 1 \pmod m \quad \text{if} \quad m > 2; \end{aligned}$$

so

$$F_{z+1} \not\equiv \pm 1 \pmod{m}.$$
$$F_{z+1}^3 = F_{z+1}^2 F_{z+1} \equiv -F_{z+1} \pmod{m};$$
$$F_{z+1}^4 = [F_{z+1}^2]^2 \equiv 1 \pmod{m},$$

and

$$T(m) = 4.$$

Lemma 2.2: $$F_{k-1} \equiv 1 \pmod{m}.$$

Proof: $$F_{k-1} = F_{k+1} - F_k \equiv F_1 - 0 \pmod{m}$$
$$\equiv 1 \pmod{m}.$$

3. THEOREMS

Theorem 3.1: If $\ell \neq 1$ and $F_{z+1}^{\frac{1}{2}\ell} \equiv -1 \pmod{m}$, then

$$F_r + F_{\frac{1}{2}\ell z+r} \equiv 0 \pmod{m} \quad \text{for all} \quad r > 0.$$

Proof: $\ell = T(m)$ which takes only the values $1, 2, 4$ (Lemma 2.1). But $\ell \neq 1$ (given). Therefore ℓ is even. Therefore, $F_{z+1}^{\frac{1}{2}\ell}$ exists and is unique. Moreover,

$$F_{\frac{1}{2}\ell z+r} \equiv F_{z+1}^{\frac{1}{2}} F_r \pmod{m} \quad \text{(see Eq. (8) of [4])}$$
$$\equiv -F_r \pmod{m} \quad \text{as} \quad F_{z+1}^{\frac{1}{2}\ell} \equiv -1$$
$$\therefore F_r + F_{\frac{1}{2}\ell z+r} \equiv 0 \pmod{m}.$$

NOTE. (i) Conversely, if for $\ell \neq 1$ we are given that

$$F_r + F_{\frac{1}{2}\ell z+r} \equiv 0 \pmod{m},$$

for all r, this congruence must hold for $r = 1$.

$$\therefore 1 = F_1 \equiv -F_{\frac{1}{2}\ell z+1} \pmod{m}$$
$$\equiv -F_{z+1}^{\frac{1}{2}\ell} F_1 \pmod{m}$$
$$\equiv -F_{z+1}^{\frac{1}{2}\ell}.$$

On the other hand, it is possible for

$$F_r + F_{\frac{1}{2}\ell z+r}$$

to be congruent to zero for some particular r without $F_{z+1}^{\frac{1}{2}\ell}$ being congruent to -1. Thus, when $m = 12$,

$$F_{12} = 144 \equiv 0 \pmod{12} \quad \text{and} \quad z = 12.$$
$$F_{z+1} = F_{13} = 233 \equiv 5 \pmod{12}$$
$$\therefore \ell = 2$$
$$\therefore F_{z+1}^{\frac{1}{2}\ell} = F_{13} \not\equiv -1 \pmod{12}.$$

Despite this,

$$F_3 + F_{\frac{1}{2}\ell z+3} = F_3 + F_{15} = 2 + 610 = 612 \equiv 0 \pmod{12}.$$

(ii) When $\ell = 1$ the situation is very untidy. If z is odd, $F_{\frac{1}{2}\ell z+r}$ does not exist. Even when z is even, we have trouble with $F_{z+1}^{\frac{1}{2}\ell}$. As $\ell = 1$, $F_{z+1} \equiv 1 \pmod{m}$. Therefore

$$F_{z+1}^{\frac{1}{2}} = \sqrt{F_{z+1}} \equiv \sqrt{1} = \pm 1$$

(and possibly other values as well). -1 is always a possible value for $F_{z+1}^{\frac{1}{2}}$, but never the exclusive value.

(iii) Although -1 is always a possible value for $F_{z+1}^{\frac{1}{2}\ell}$ $(\ell = 1)$, it is not necessarily true that

$$F_r + F_{\frac{1}{2}\ell z+r} \equiv 0 \pmod{m} \quad \text{for all} \quad r > 0.$$

Thus, when $m = 4$, $z = 6$.

$$\therefore F_{z+1} \equiv 1 \pmod{m}, \quad \therefore \ell = 1.$$
$$\therefore F_2 + F_{\frac{1}{2}z+2} = F_2 + F_5 = 6 \equiv 2 \pmod{4}.$$

Theorem 3.2: $F_r + (-1)^r F_{k-r} \equiv 0 \pmod{m}$.

Proof: $-F_k \equiv 0 = F_0$ and $F_{k-1} \equiv 1 = F_1 \pmod{m}$, by Lemma 2.2

$$-F_{k-2} = -F_k + F_{k-1} \equiv F_0 + F_1 \equiv F_2 \pmod{m}.$$

It follows by induction on k that

$$\begin{aligned}(-1)^{r-1}F_{k-r} &= (-1)^{r-1}F_{k-r+2} + (-1)^r F_{k-r+1}\\ &\equiv F_{r-2} + F_{r-1} \pmod{m}\\ &\equiv F_r \pmod{m},\end{aligned}$$

which gives the required result.

4. CONGRUENCES MODULO m^2

Here we use the results (see Hoggatt [3])

(4.1) $$F_{nr+1} = F_{(n-1)r}F_r + F_{(n-1)r+1}F_{r+1}$$

and

(4.2) $$F_{2n+1} = F_n^2 + F_{n+1}^2 .$$

If $a \pmod{m} \equiv F_{z+1} \equiv b \pmod{m^2}$, then b is of the form $Bm + a$, for some B. For example, $F_5 \equiv 0 \pmod{5}$, $3 \pmod{5} \equiv F_6 \equiv 8 \pmod{5^2}$, and $8 = 1 \times 5 + 3$.

Using $F_z \equiv 0 \pmod{m}$ and (4.1) and (4.2) we find

$$F_{2z+1} \equiv F_{z+1}^2 \pmod{m^2} \equiv b^2 \pmod{m^2},$$

and

$$F_{3z+1} \equiv F_{2z+1}F_{z+1} \pmod{m^2} \equiv b^3 \pmod{m^2},$$

which, by the use of (4.1), can be generalized to

(4.3) $$F_{nz+1} \equiv b^n \pmod{m^2}.$$

Furthermore, since $F_z = Am$ for some A, then

$$F_{z-1} \equiv b - Am \pmod{m^2}$$

and

$$\begin{aligned}F_{2z} &= F_{z-1}F_z + F_zF_{z+1}\\ &\equiv (b - Am)Am + Amb \pmod{m^2}\\ &\equiv 2bAm \pmod{m^2}.\end{aligned}$$

Also,

$$\begin{aligned}F_{3z} &= F_{2z-1}F_z + F_{2z}F_{z+1} \quad \text{(from (4.1))}\\ &\equiv (b^2 - 2bAm)Am + 2bAm \cdot b \pmod{m^2}\\ &\equiv 3b^2Am \pmod{m^2}.\end{aligned}$$

Similarly, $F_{4z} \equiv 4b^3Am \pmod{m^2}$. Thus

(4.4) $$F_{nz} \equiv nb^{n-1}Am \pmod{m^2}.$$

When $F_{nz} \equiv 0$ the congruence $nb^{n-1}A \equiv 0 \pmod{m}$ reduces to $nA \equiv 0 \pmod{m}$, because, from (4.3) and (4.4), if b and m have any factor in common, so have F_{nz} and F_{nz+1}, which is impossible as adjacent Fibonacci numbers are always co-prime. Thus, if we solve $nA \equiv 0 \pmod{m}$ for n, then $Z = nz$ gives that F_Z which is zero $\pmod{m^2}$.

Let us apply these methods to find which Fibonacci numbers are divisible by convenient powers of 10. Instead of working with $m = 10$, we shall find the equations simpler if we write $10 = m_1 \cdot m_2$, where $m_1 = 2$, $m_2 = 5$, and $100 = 2^2 \cdot 5^2$. $m_1 = 2$, $z = 3$, $F_3 = 1 \cdot 2$ and so $A = 1$. The equation $nA \equiv 0 \pmod{m}$ reduces to $n \equiv 0 \pmod{2}$, which gives $n = 2$, so that $Z = 2z = 6$. Similarly with $m_2 = 5$, $z = 5$, and we find that $Z = 5z = 25$.

If we take $m_1 = 4$, $z = 6$, $F_6 = 2 \cdot 4$ and so $A = 2$. Thus $2n \equiv 0 \pmod{4}$ which gives $n = 2$ and $Z = 2z = 12$. Similarly, with $m_2 = 25$, $z = 25$ and $F_{25} = 75025 = 3001 \cdot 25$ which yields $A \equiv 1 \pmod{25}$. So $n = 25$ and $Z = 25z = 625$.

Relying on the known result that the period of divisibility by m_1m_2 (m_1, m_2 co-prime) is given by $D(m_1m_2) = LCM(z_1, z_2)$ (see Wall [6]), we get the results:

$LCM(3,5) = 15$, and so F_{15} is the first Fibonacci number to be divisible by 10. $lcm(6,25) = 150$, and so F_{150} is divisible by 100. $LCM(12,625) = 7,500$ and so F_{7500} is divisible by 10^4.

This has been an exercise in finding the z numbers. By an extension of the argument we can produce the corresponding k numbers—the period of recurrence of the Fibonacci numbers (mod m^2).

REFERENCES

1. S.N. Collings, "Fibonacci Numbers," *Mathematics Teaching,* No. 52 (1970), p. 23.
2. D.E. Daykin and L.A.G. Dresel, "Factorization of Fibonacci Numbers," *The Fibonacci Quarterly,* Vol. 8, No. 1 (February 1970), pp. 23-30.
3. V.E. Hoggatt, Jr., *Fibonacci and Lucas Numbers,* Houghton-Mifflin, Boston, 1969, p. 59.
4. A.G. Marshall, "Fibonacci, Modulo n," *Mathematics Teaching,* No. 46 (1969), p. 29.
5. J. Vinson, "The Relation of the Period Modulo to the Rank of Apparition of m in the Fibonacci Sequence," *The Fibonacci Quarterly,* Vol. 1, No. 2 (April 1963), pp. 37–45.
6. D.D. Wall, "Fibonacci Series Modulo m," *American Math. Monthly,* Vol. 67 (1960), pp. 525–532.
7. O. Wyler, "On Second-Order Recurrences," *American Math. Monthly,* Vol. 72 (1965), pp. 500–506.

****

[Continued from page 350.]

$$F_k(x) = \sum_{j=0}^{[k/2]} (-1)^j e^j \frac{k}{k-j} \binom{k-j}{j} g_{k-2j}((-1)^j x) . \tag{5}$$

Write

$$\begin{cases} h_k(x) = (1 - a_k x + (-1)^k x^2) g_k(x) \\ c_k \quad = [(r-sb)a]^k + [(sa-r)b]^k . \end{cases} \tag{6}$$

Following Riordan [6], with $a_0 = 2$ and $h_0(x) = 1 - x$, we eventually derive

$$\begin{cases} c_1 + s\sqrt{5}\,x = h_1(x) \\ c_2 - x(2e+5s^2) = h_2(x) - 2e\left\{h_0(-x) - (a_0+a_2)xg_0(-x)\right\} \\ c_3 + s\sqrt{5}\,x(3e+5s^2) = h_3(x) - 3e\left\{h_1(-x) - (a_1+a_3)xg_1(-x)\right\} \\ c_4 - x(2e^2+20s^2e+25s^4) = h_4(x) - 4e\left\{h_2(-x) - (a_2+a_4)xg_2(-x)\right\} \\ \qquad\qquad + 2e^2\left\{h_0(x) - (a_4-a_0)xg_0(x)\right\} \\ c_5 - e_1 = h_5(x) - 5e\left\{h_3(-x) - (a_3+a_5)xg_3(-x)\right\} + 5e^2\left\{h_1(x) - (a_5-a_1)xg_1(x)\right\} \end{cases} \tag{7}$$

where

$$e_1 = 2r^5 - 5r^4s + 30r^2s^2 - 40r^2s^3 + 35rs^4 - 10s^5 .$$

Substituting values of $a_k = a^k + b^k$, we have

$$\begin{cases} h_1(x) = \sqrt{5}\,(r+sx) \\ h_2(x) = 5(r^2 - s^2x) - 10exg_0(-x) \\ h_3(x) = 5\sqrt{5}\,(r^3+s^3x) - 15exg_1(-x) \\ h_4(x) = 25(r^4 - s^4x) - 40exg_2(-x) + 50e^2xg_0(x) \\ h_5(x) = 25\sqrt{5}\,(r^5+s^5x) - 75exg_3(-x) + 125e^2xg_1(x) . \end{cases} \tag{8}$$

These functions lead back to (2).

[Continued on page 362.]