THE FIBONACCI RATIOS F_{k+1}/F_k MODULO p

LAWRENCE SOMER
University of Illinois, Champaign, Illinois 61820

It is well known that the ratios F_{k+1}/F_k converge to ϕ, the golden ratio. These fractions are alternately greater than and less than ϕ. However, interesting relationships also arise if we consider these ratios reduced modulo p, where p is an odd prime.

Before proceeding further, we will need a few definitions. Let R_k be the Fibonacci ratio F_{k+1}/F_k. Let $z(p)$ be the restricted period of the Fibonacci series reduced modulo p—that is, $F_{z(p)}$ is the first term $\equiv 0 \pmod p$ in the series. Let $\omega(p)$ be the period of the Fibonacci sequence modulo p and let

$$\beta(p) = \omega(p)/z(p).$$

If $z(p) \equiv 2 \pmod 4$, $\beta(p) = 1$; if $z(p) \equiv 4 \pmod 8$, $\beta(p) = 2$; and if $z(p) \equiv 1 \pmod 2$, $\beta(p) = 4$. See [1]. Further, let us agree to ignore all ratios modulo p which have 0 as a denominator.

Then, the Fibonacci ratios reduced modulo p repeat in periods of length $z(p) - 1$. This follows since the terms $F_{kz(p)+1}$ to $F_{(k+1)z(p)}$ are constant multiples of the first $z(p)$ terms. Furthermore, no two ratios within a period repeat, since this would imply that a term of the Fibonacci series preceding $F_{z(p)}$ was congruent to 0 modulo p.

Thus, if $z(p) = p + 1$, all the residues will be represented in the period of Fibonacci ratios reduced modulo p. The fact that none of these ratios repeat is an easy way of showing that $z(p) \leqslant p + 1$. A necessary but not sufficient condition for $z(p)$ to equal $p + 1$ is that $(5/p) = -1$ and $\beta(p) = 2$, which is equivalent to saying that $p \equiv 3$ or $7 \pmod{20}$. See [1]. For primes such as 3, 7, 23, and 43, $z(p)$ does in fact equal $p + 1$.

The Fibonacci ratios reduced modulo 7 are shown below:

k	F_k	R_{k-1}
1	1	
2	1	$1/1 \equiv 1 \pmod 7$
3	2	$2/1 \equiv 2 \pmod 7$
4	3	$3/2 \equiv 5 \pmod 7$
5	5	$5/3 \equiv 4 \pmod 7$
6	1	$1/5 \equiv 3 \pmod 7$
7	6	$6/1 \equiv 6 \pmod 7$
8	0	$0/6 \equiv 0 \pmod 7$

Theorem 1. $R_{z(p)-n} \equiv 1 - R_n \pmod p$ for $1 \leqslant n \leqslant z(p) - 1$.

Proof. This is true for $n = 1$, since $R_1 = 1/1 \equiv 1 \pmod p$ and $R_{z(p)-1} \equiv 0 \pmod p$.

Now assume that the hypothesis is true up to $n = k$. Let $R_k = r$. Then

$$\frac{F_{k+1}}{F_k} \equiv r \qquad \text{and} \qquad \frac{F_{z(p)-k+1}}{F_{z(p)-k}} \equiv 1 - r \pmod p$$

Thus, $F_{k+1} \equiv rF_k \pmod p$.

$$R_{k+1} = \frac{F_{k+2}}{F_{k+1}} = \frac{F_{k+1}+F_k}{F_{k+1}} \equiv \frac{(r+1)F_k}{rF_k} \equiv \frac{r+1}{r} \pmod p.$$

Also,

$$R_{z(p)-k-1} \equiv \frac{F_{z(p)-k}}{F_{z(p)-k-1}} \equiv \frac{F_{z(p)-k}}{F_{z(p)-k+1} - F_{z(p)-k}} \equiv \frac{F_{z(p)-k}}{(1-r)F_{z(p)-k} - F_{z(p)-k}}$$

$$\equiv \frac{F_{z(p)-k}}{-rF_{z(p)-k}} \equiv \frac{-1}{r} \pmod p.$$

But

$$\frac{r+1}{r} \equiv 1 - \left(\frac{-1}{r}\right) \pmod p$$

and we are done.

Theorem 2. $R_n \cdot R_{z(p)-n-1} \equiv -1 \pmod p$ for $1 \leqslant n \leqslant z(p) - 2$.

Proof. $R_1 \equiv 1$ and $R_2 \equiv 2 \pmod p$. By the previous theorem,

$$R_{z(p)-2} \equiv 1 - 2 \equiv -1 \equiv \frac{-1}{R_1} \pmod p.$$

Thus, the theorem holds for $n = 1$. The rest of the proof by induction is similar to the previous proof.

The remainder of this paper will be devoted to investigating what residues appear and do not appear among the Fibonacci ratios reduced modulo p. We will not consider such trivial residues as 2/1 or 3/2. By Theorem 1, if $z(p)$ is even then the ratio $R_{\frac{1}{2}z(p)}$ will be $\equiv \frac{1}{2} \pmod p$. If $z(p)$ is odd, then Theorem 1 implies that ½ will not appear among the Fibonacci ratios modulo p. Thus, if $\beta(p) = 1$ or 2, ½ appears among the Fibonacci ratios and if $\beta(p) = 4$, ½ will not be among the Fibonacci ratios modulo p.

By Theorem 2, if $z(p)$ is odd $R_{\frac{1}{2}(z(p)-1)}$ will be congruent to one of the square roots of $-1 \pmod p$. If $z(p)$ is even, no square roots of -1 will show up among the Fibonacci ratios reduced modulo p.

Combining theorems 1 and 2, we see that no solution of the congruence

$$1 - k \equiv \frac{-1}{k} \pmod p$$

will appear among the Fibonacci ratios modulo p. Solving for k, we see that

$$k \equiv \frac{1 \pm \sqrt{5}}{2} \pmod p$$

if $(5/p) = 0$ or 1. It turns out that for certain primes such as 11, 19, and 31, $z(p) = p - 1$, and every residue but

$$\frac{1 \pm \sqrt{5}}{2}$$

appears among the Fibonacci ratios modulo p. A necessary but not sufficient condition for this to occur is that $p \equiv 11$ or $19 \pmod{20}$.

We are now ready to summarize our results:

For all primes if the residue r appears among the Fibonacci ratios modulo p, then $1 - r$ and $-1/r$ will also appear.

$p = 5$: All residues except $\frac{1}{2} \equiv 3 \pmod 5$ will appear.

$p \equiv 3$ or $7 \pmod{20}$: All residues might appear since $z(p)$ might equal $p + 1$. In any case, the residue ½ will appear.

$p \equiv 11$ or $19 \pmod{20}$: The residue ½ appears. The residues

$$\frac{1 \pm \sqrt{5}}{2} \pmod p$$

do not appear. All other residues could appear since $z(p)$ might equal $p - 1$.

$p \equiv 13$ or 17 (mod 20): The residue ½ does not appear. Exactly one square root of -1 appears.

$p \equiv 1$ or 9 (mod 20) and $\beta(p) = 1$ or 2: The residue ½ appears. Both square roots of -1 and the residues

$$\frac{1 \pm \sqrt{5}}{2} \pmod p$$

do not appear.

$p \equiv 1$ or 9 (mod 20) and $\beta(p) = 4$: The residues ½ and

$$\frac{1 \pm \sqrt{5}}{2} \pmod p$$

do not appear. Exactly one square root of $-1 \pmod p$ appears.

REFERENCE

1. John H. Halton, "On the Divisibility Properties of Fibonacci Numbers," *The Fibonacci Quarterly*, Vol. 4, No. 3 (Oct. 1966), pp. 217–241.

****

[Continued from P. 321.]

If $(a,b) = 1$, then

$$(a^2/b^2) = 1,$$
$$(-a^2/b^2) = 1,$$
$$(a^2/-b^2) = 1,$$
$$(-a^2/-b^2) = -1;$$

$$(a/b^2) = 1,$$
$$(-a/b^2) = 1,$$
$$(a/-b^2) = (a/-1),$$
$$(-a/-b^2) = -(a/-1);$$

$$(a^2/b) = 1,$$
$$(-a^2/b) = (-1/b),$$
$$(a^2/-b) = 1,$$
$$(-a^2/-b) = -(-1/b);$$

$$(a/b) = (a/b),$$
$$(-a/b) = (a/b)(-1/b),$$
$$(a/-b) = (a/b)(a/-1),$$
$$(-a/-b) = -(a/b)(a/-1)(-1/b).$$

It remains to evaluate $(a/-1)$. Since $(-a^2/-1) = -1$, therefore $(a/-1) = -(-a/-1)$. This means that $(a/-1)$ cannot be defined in terms of an integer. Either $(a/-1) = 1$ if and only if a is positive or $(a/-1) = 1$ if and only if a is negative. The choice of alternative is dictated by the fact that $(1/-1) = 1$ and $(-1/-1) = -1$. Therefore, $(a/-1) = 1$ if and only if a is positive.

(See Tables 1 through 4.)

[Continued on P. 328.]