THE FIBONACCI GROUP AND A NEW PROOF THAT $F_{p-(5/p)} \equiv 0 \pmod p$

LAWRENCE E. SOMER
1266 Parkwood Drive, No. Merrick, New York

It is fairly well known that $F_{p-(5/p)} \equiv 0 \pmod p$, where p is an odd prime; F_p is the p^{th} Fibonacci number, and $(5/p)$ is the Legendre symbol. Three different proofs of this theorem are given in [1], [2], and [3].

My method of proof of this theorem is based on the restricted periods of generalized Fibonacci sequences reduced modulo p and the existence of what I call Fibonacci groups modulo certain primes.

Look at the congruence: $a + ax \equiv ax^2 \pmod p$. This implies $ax^{n-1} + ax^n \equiv ax^{n+1} \pmod p$. Solving for x: $x \equiv (1 \pm \sqrt{5})/2 \pmod p$. Thus we can solve for x iff 5 is a quadratic residue of $p > 2$. If $a \equiv 1 \pmod p$, the recursion relation: $a + ax \equiv ax^2 \pmod p$ will generate the successive terms: $(1, x, x^2, \cdots, x^n, \cdots)$, and we will have a Fibonacci group.

As an example of a Fibonacci group, solve $x \equiv (1 \pm \sqrt{5})/2 \pmod{11}$. We see $x \equiv (1 \pm 4)/2 \pmod{11} \equiv 4$ or $8 \pmod{11}$. If $x \equiv 4 \pmod{11}$, we get the group $(1, 4, 5, 9, 3)$ and if $x \equiv 8 \pmod{11}$, we obtain the group $(1, 8, 9, 6, 4, 10, 3, 2, 5, 7)$. In each case each term is the sum of the preceding two terms (mod 11) and is a constant multiple of the preceding term.

Definitions. Let $\{H_n\}$ be a generalized Fibonacci sequence (hereafter called G. F. S.) reduced modulo p; $H_1 = a$, $H_2 = b$; $H_n \equiv H_{n-1} + H_{n-2} \pmod p$; p an odd prime.

$\{H_n\}$ is periodic modulo p. Let $\mu(a, b, p)$ be the period of the G. F. S. which begins with (a,b) modulo p. That is, $\mu(a, b, p)$ is the least positive integer n such that $H_n \equiv H_0 \equiv H_2 - H_1$ and $H_{n+1} \equiv H_1 \pmod p$.

Also, let $\alpha(a, b, p)$ be the restricted period of $\{H_n\}$ (mod P). Thus, $\alpha(a, b, p)$ is the least positive integer m such that $H_m \equiv sH_0$ and $H_{m+1} \equiv sH_1 \pmod p$ for some s. Let $s(a, b, p) \equiv s \pmod p$; $s(a, b, p)$ will be called the multiplier of $\{H_n\}$ (mod p).

Theorem 1. If the initial pair (a,b) of $\{H_n\} \not\equiv (0, 0)$, $(a, a(1 + \sqrt{5})/2)$, or $(a, a(1 - \sqrt{5})/2) \pmod p$, then $\alpha(a, b, p) = \alpha(1, 1, p)$, $s(a, b, p) = s(1, 1, p)$, and $\mu(a, b, p) = \mu(1, 1, p)$.

Proof. Write out the Fibonacci series reduced modulo p from F_1 to $F_{\mu(1,1,p)}$. There will be $\mu(1, 1, p)$ consecutive pairs in this sequence if we count $(F_{\mu(p)}, F_1) \equiv (0, 1) \pmod p$ as a consecutive pair of terms. If a pair (c,d) does not appear in this sequence, start another G. F. S. with this pair up to $H_{\mu(c,d,p)}$. No pair will be repeated since each pair determines each term that follows and precedes by the recursion relation, and each G. F. S. is periodic modulo p.

One can continue this process until all the p^2 possible pairs are used up. We shall need three lemmas to finish the proof.

Lemma 1. Any linear combination of two G. F. S.'s yields a G. F. S.

Proof. Let $\{G_n\}$, $\{H_n\}$, be two G. F. S's. Then

$$rG_{n-1} + sH_{n-1} + rG_n + sH_n = r(G_{n-1} + G_n) + s(H_{n-1} + H_n) = rG_{n+1} + sH_{n+1} ,$$

and the recursion relation is still satisfied.

Now, we can express any pair of terms (a,b) as $(b - a)$:

$$(F_0, F_1) + a(F_1, F_2) = (b - a)(0,1) + a(1,1) = (b - a, a)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} .$$

Lemma 2. For all G. F. S. $\{H_n\}$,

$$(H_{\alpha(1,1,p)+1}, H_{\alpha(1,1,p)+2}) \equiv s(1,1,p)(a,b); \quad a = H_1, \quad b = H_2 ,$$

Proof. Let $\alpha(1, 1, p) = n$. Then

$$(F_n, F_{n+1}) \equiv s(1,1,p)(F_0, F_1)$$

and

$$(F_{n+1}, F_{n+2}) \equiv s(1,1,p)(F_1, F_2) \pmod p,$$

by definition. But

$$\begin{aligned}(H_{n+1}, H_{n+2}) &\equiv (b - a)(F_n, F_{n+1}) + a(F_{n+1}, F_{n+2}) \\ &\equiv (b - a)s(1,1,p)(F_0, F_1) + (a)s(1,1,p)(F_1, F_2) \equiv s(1,1,p)(a,b) \pmod p.\end{aligned}$$

Corollary: $(H_{\mu(1,1,p)+1}, H_{\mu(1,1,p)+2}) \equiv (a,b)$.

This proof is exactly the same as that for Lemma 2. It is interesting to note that this corollary implies that length of a Fibonacci group $\le \mu(1,1,p)$.

Lemma 3. If $b \not\equiv a(1 \pm \sqrt{5})/2$, then $\alpha(a,b,p) = \alpha(1,1,p)$. (Note that if $(a,b) = (F_1, F_2) = (1,1)$, then $b \not\equiv a(1 \pm \sqrt{5})/2 \pmod p$ since this implies that $\sqrt{5} \equiv \pm 1 \pmod p$, which is false for $p \ge 3$.)

Proof. Assume that this assertion is false for some $\{H_n\}$, where $b \not\equiv a(1 \pm \sqrt{5})/2$. Let $\alpha(a,b,p) = n$. By Lemma 2, $n < \alpha(1,1,p)$. Then

$$(H_{n+1}, H_{n+2}) \equiv s(a,b,p)(a,b) \equiv (b - a)(F_n, F_{n+1}) + a(F_{n+1}, F_{n+2}) \pmod p .$$

Let $F_{n+1} = x \cdot F_1 = x$ and $F_{n+2} = y \cdot F_2 = y$; $x \neq y$ since $n < \alpha(1,1,p)$. Then

$$\frac{H_{n+2}}{H_{n+1}} = \frac{s(a,b,p)b}{s(a,b,p)a} \equiv \frac{b}{a} \equiv \frac{(b-a)F_{n+1} + aF_{n+2}}{(b-a)F_n + aF_{n+1}}$$

$$\equiv \frac{(b-a)F_{n+1} + aF_{n+2}}{(b-a(F_{n+2} - F_{n+1}) + aF_{n+1}} \equiv \frac{(b-a)x + ay}{(b-a)(y-x) + ax} \pmod{p}.$$

Thus,

$$\frac{b}{a} \equiv \frac{bx - ax + ay}{by - ay - bx + 2ax} \pmod{p}.$$

I claim that neither a nor $(by - ay - bx + 2ax \equiv H_{n+1}) \equiv 0 \pmod{p}$. If $a \equiv 0$, then $(a,b) \equiv (0,0)$ or $(a,b) \equiv (0,k)$, $k \not\equiv 0 \pmod{p}$. The pair $(0,0)$ is excluded by hypothesis, and if $(a,b) \equiv (0,k)$, $\{H_n\}$ is a non-zero multiple of the Fibonacci sequence. Since the residues modulo p form a field, there are no divisors of 0 and a multiple of the Fibonacci sequence will have the same restricted period. Therefore $n = \alpha(1,1,p)$ and we have a contradiction. If $H_{n+1} \equiv 0 \pmod{p}$, the same argument leads to a contradiction.

The congruence

$$\frac{b}{a} \equiv \frac{bx - ax + ay}{by - ay - bx + 2ax} \pmod{p}$$

leads to the congruence

$$b^2(y - x) - ab(y - x) - a^2(y - x) \equiv 0 \pmod{p}.$$

Dividing through by the non-zero $(y - x)$ and solving for b, we obtain $b \equiv a(1 \pm \sqrt{5})/2$, a contradiction. Q.E.D.

Corollary. If $b \not\equiv a(1 \pm \sqrt{5})/2$, then $s(a,b,p) = s(1,1,p)$ and $\mu(a,b,p) = \mu(a,b,p)$. This follows from Lemma 2, its corollary and Lemma 3.

With the help of the three lemmas and their corollaries, Theorem 1 is now proved.

We are now ready to prove the main theorem that $F_{p-(5/p)} \equiv 0 \pmod{p}$. Of the p^2 possible pairs of terms which appear in some G.F.S. reduced modulo p, one pair $(0,0)$ forms the trivial sequence $(0, 0, 0, \cdots)$. We will now look at the $p^2 - 1$ pairs remaining.

If $(5/p) = 1$, then there are two solutions to the congruence: $x \equiv (1 \pm \sqrt{5})/2$, and we can form two Fibonacci groups. By Lagrange's theorem, each group has length $(p-1)/k_i$, $(i = 1, 2)$. If we count the k_i non-zero multiples of each group, there will be $2(p-1)$ pairs of terms in some non-zero multiple of a Fibonacci group. That leaves $p^2 - 1 - 2(p-1) = (p-1)^2$ pairs remaining.

We will say that two restricted periods belong to the same equivalence class if some pair of consecutive terms of one restricted period is a non-zero multiple of a pair of another restricted period reduced modulo p. In each equivalence class, there are $p - 1$ non-zero multiples of each restricted period. Suppose there are k equivalence classes of restricted periods of length $\alpha(1,1,p)$. Then if $(5/p) = 1$, there will be $(p-1)^2$ pairs in these equivalence classes: $(p-1)(k) \cdot \alpha(1,1,p) = (p-1)^2$, and $\alpha(1,1,p) = (p-1)/k$. Since there are no divisors of $0 \pmod p$, only terms which are multiples of $(p-1)/k$ will be $\equiv 0 \pmod p$. In particular, $F_{p-1} \equiv 0 \pmod p$.

If $(5/p) = 0$, then $p = 5$ and $\sqrt{5} \equiv 0 \pmod p$. Thus, there is only one root of the congruence: $x \equiv (1 \pm \sqrt{5})/2 - x \equiv 3 \bmod 5$. This leads to the Fibonacci group $(1, 3, 4, 2)$. Excluding the trivial pair $(0,0)$, there are $p^2 - 1 - (p-1)$ pairs which are not members of multiples of Fibonacci groups $\pmod p$. Then $p(p-1) = (p-1)(k) \cdot \alpha(1,1,p)$, and $\alpha(1,1,p) = p/k$. This implies that $F_p \equiv 0 \pmod p$.

If $(5/p) = -1$, there are no Fibonacci groups $\pmod p$, and $p^2 - 1 = (p-1)(k)\alpha(1,1,p)$. Thus, $\alpha(1,1,p) = (p+1)/k$, and $F_{p+1} \equiv 0 \pmod p$. Q. E. D.

This theorem can easily be generalized. Let us define a Fibonacci-like sequence $\{J_n\}$ as one which satisfies the recursion relation: $J_{n+1} = aJ_n + bJ_{n-1}$; a, b positive integers. In accordance with the notation of Robert P. Backstrom [4], I will call the Fibonacci-like sequence beginning with $(1,a)$ the primary sequence. If $b \not\equiv 0 \pmod p$, then by the recurrence relation $bJ_0 \equiv j_2 - aJ_1 \equiv a - a(1) \equiv 0$, which implies that $J_0 \equiv 0 \pmod p$. Thus, if $b \not\equiv 0 \pmod p$, the primary sequence $\{J_n\}$ will be absolutely periodic and $J_{\alpha(p)}$ will be $\equiv 0 \pmod p$. It should be noted that only in multiples of a primary sequence will all but a finite number of primes (excepting possibly only those primes that divide b) divide some positive term of the sequence.

We can form a Fibonacci-like group analogous to the Fibonacci group by solving the congruence: $bc + acx \equiv cx^2 \pmod p$ for x; $x \equiv (a \pm \sqrt{a^2 + 4b})/2$. As an example of such a group, if $a = 1$, $b = 3$, then a Fibonacci-like group exists iff $(a^2 + 4b/p) = (13/p) = 0$ or 1, if $p = 17$, then a solution of $x \equiv (1 \pm \sqrt{13})/2 \equiv (1 \pm 8)/2 \pmod{17}$ is $x \equiv 13 \bmod 17$, and this gives rise to the Fibonacci-like group $(1, 13, 16, 4)$.

As before, any arbitrary Fibonacci-like sequence is the linear combination of two primary sequences. If (c,d) are two consecutive terms of a Fibonacci-like sequence and $\{J_n\}$ is a primary sequence, then

$$(c,d) = (d - ac)(J_0, J_1) + c(J_1, J_2) = (d - ac)(0,1) + c(1,a) = (d - ac, c)\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}.$$

Let $a^2 + 4b = k$. If $b \not\equiv 0 \pmod p$, p an odd prime, then by an argument analogous to the one above, we can prove the theorem: $J_{p-(k/p)} \equiv 0 \pmod p$ if $\{J_n\}$ is the primary sequence.

If $a \not\equiv 0 \pmod p$, $b \equiv 0 \pmod p$, then solving the congruence:

$$x \equiv (a \pm \sqrt{a^2 + 4b})/2 \equiv (a \pm \sqrt{a^2})/2 \pmod p,$$

we see that $x \equiv a$ or $0 \pmod p$. Thus, the primary sequence generated by $(1,a)$ will be a Fibonacci-like group and no positive term will be divisible by p.

[Continued on page 354.]