FIBONACCI-LIKE GROUPS AND PERIODS OF FIBONACCI-LIKE SEQUENCES

LAWRENCE SOMER
1266 Parkwood Drive, North Merrick, New York 11566

The purpose of this paper is to investigate Fibonacci-like groups and use them to show that for any odd prime p, there are Fibonacci-like sequences, in fact an infinite number of them, with a maximal period modulo p. At the conclusion of this paper, we will present a program to show how one might apply Fibonacci-like groups to problems concerning primitive roots modulo an odd prime. One of our main results will be to prove that the exponent to which any non-zero residue r of an odd prime p belongs is equal to either the period or one-half the period modulo p of a Fibonacci-like sequence, except when both $p \equiv 1 \pmod 4$ and $r \equiv \pm\sqrt{-1} \pmod p$. We will give a proof of this theorem and draw some consequences. To continue, we will need a few definitions.

Definition 1. A primary Fibonacci-like sequence $\{J_n\}$, hereafter called a P.F.L.S., is one which satisfies the recursion relation: $J_{n+1} = aJ_n + bJ_{n-1}$ for some non-negative integers, a, b, and for which $J_0 = 0$, $J_1 = 1$, and $J_2 = a$.

Definition 2. A generalized Fibonacci-like sequence, hereafter called G.F.L.S., is a Fibonacci-like sequence $\{K_n\}$ in which K_0 and K_1 are arbitrary non-negative integers.

Definition 3. $\mu(a, b, p)$ is the period modulo p, p an odd prime, of a P.F.L.S. in which

$$J_{n+1} = aJ_n + bJ_{n-1}.$$

It is the first positive integer n such that $J_n \equiv 0 \pmod p$ and $J_{n+1} \equiv J_1 \equiv 1 \pmod p$.

Definition 4. $\alpha(a, b, p)$, called the restricted period of a P.F.L.S. modulo p, is the least positive integer m such that

$$J_m \equiv sJ_0 \equiv 0 \qquad \text{and} \qquad J_{m+1} \equiv sJ_1 \equiv s \pmod p$$

for some residue s. Then $s(a, b, p) = s$ will be called the multiplier of the P. F. L. S. modulo p.

Definition 5. $\beta(a, b, p)$ is the exponent of $s(a, b, p) \pmod p$. It is equal to $\mu(a, b, p)/\alpha(a, b, p)$.

The next fact that we will need is that if $(a^2 + 4b/p) = 0$ or 1, where (p/q) is the Legendre symbol, then the period of the G.F. L.S. modulo p, beginning with either

$$(K_0 \equiv 1,\ K_1 \equiv (a + \sqrt{a^2 + 4b})/2) \qquad \text{or} \qquad (K_0 \equiv 1,\ K_1 \equiv (a - \sqrt{a^2 + 4b})/2),$$

forms a group under multiplication (mod p). The G.F.L.S., reduced modulo p, beginning with

$$(1, (a + \sqrt{a^2 + 4b})/2)$$

will be designated by $\{M_n\}$ and the G.F.L.S. beginning with

$$(1, (a - \sqrt{a^2 + 4b})/2)$$

by $\{M'_n\}$. The specific generalized Fibonacci sequence beginning with

$$(1, (1 + \sqrt{5})/2), \qquad \text{and} \qquad (1, (1 - \sqrt{5})/2),$$

reduced modulo p, will be designated by $\{H_n\}$ and $\{H'_n\}$, respectively. Generalized Fibonacci sequences satisfy the same recursion relation as the Fibonacci sequence.

To prove that these form multiplicative groups modulo p, note that the congruence:

$$bc + acx \equiv cx^2 \pmod p$$

leads to the congruence:

$$bcx^{n-1} + acx^n \equiv cx^{n+1} \pmod{p}.$$

This has the solutions

$$x \equiv \tfrac{1}{2}a \pm \tfrac{1}{2}\sqrt{a^2 + 4b} \pmod{p}.$$

Letting $c = 1$, we see immediately that we obtain the group generated by the powers of x. These sequences will be called Fibonacci-like groups modulo p and the sequences $\{H_n\}$ and $\{H'_n\}$ will be called Fibonacci-groups modulo p. Note that these sequences have both the additive structure of a Fibonacci-like sequence and the multiplicative structure of a cyclic group. For an example of a Fibonacci-like group, let $a = 1$ and $b = 3$. Then a Fibonacci-like group exists iff

$$(a^2 + 4b/p) = (13/p) = 0 \text{ or } 1.$$

If $p = 17$, then a solution of

$$x \equiv (1 \pm \sqrt{13})/2 \equiv (1 \pm 8)/2 \pmod{17}$$

is $x \equiv 13 \pmod{17}$, and this gives rise to the Fibonacci-like group (1, 13, 16, 4).

Our method of proof of the main theorem will be based on the length of the periods of special types of Fibonacci-like groups, namely those for which $b = 1$.

To demonstrate my method of proof, we will investigate the periods modulo p of the Fibonacci groups, $\{H_n\}$ and $\{H'_n\}$. Using the quadratic reciprocity formula, we can see that Fibonacci groups exist modulo p only when $p = 5$ or $p \equiv \pm 1 \pmod{10}$.

Any generalized Fibonacci sequence $\{G_n\}$ beginning with $G_0 = c$, $G_1 = d$, can be generated from the Fibonacci sequence $\{F_n\}$ by the formula:

$$G_n = (d - c)F_n + cF_{n+1}.$$

Thus, all the terms of the two Fibonacci groups $\{H_n\}$ and $\{H'_n\}$ which are $\equiv 1 \pmod{p}$ can be expressed as:

$$H_n \equiv ((1 + \sqrt{5})/2)^n \equiv ((-1 + \sqrt{5})/2)F_n + F_{n+1} \equiv 1 \pmod{p};$$

or:

$$H'_n \equiv ((1 - \sqrt{5})/2)^n \equiv (-1 - \sqrt{5})/2)F_n + F_{n+1} \equiv 1 \pmod{p}.$$

If $F_n \equiv 0 \pmod{p}$, then F_{n+1} must be $\equiv 1 \pmod{p}$ and the n^{th} term of both the sequences $\{H_n\}$ and $\{H'_n\}$ will be $\equiv 1 \pmod{p}$.

Note that the product of the n^{th} terms of the two Fibonacci groups modulo p, $p \neq 5$, is

$$((1 + \sqrt{5})/2)^n \cdot ((1 - \sqrt{5})/2)^n \equiv -1^n \pmod{p}.$$

Let us now assume either $H_n \equiv 1$ or $H'_n \equiv 1 \pmod{p}$ but that $F_n \not\equiv 0 \pmod{p}$. Then $H'_n \equiv \pm 1 \pmod{p}$ if $H_n \equiv 1 \pmod{p}$, or $H_n \equiv \pm 1 \pmod{p}$ if $H'_n \equiv 1 \pmod{p}$.

Let us assume that both H_n and H'_n are $\equiv 1 \pmod{p}$. Then

$$H_n \equiv ((-1 + \sqrt{5})/2)F_n + F_{n+1} \equiv 1 \pmod{p},$$

and

$$H'_n \equiv ((-1 - \sqrt{5})/2)F_n + F_{n+1} \equiv 1 \pmod{p}.$$

Thus,

$$H_n - H'_n \equiv 5F_n \equiv 0 \pmod{p}.$$

Since $F_n \not\equiv 0$ by assumption, $5 \equiv 0 \pmod{p}$ and p must equal 5. If $p = 5$, then

$$(1 + \sqrt{5})/2 \equiv (1 - \sqrt{5})/2 \equiv \tfrac{1}{2} \equiv 3 \pmod{5},$$

and there is only one Fibonacci group. This group is $\{1, 3, 4, 2\}$ and has a period of 4.

Now, suppose $p \neq 5$ and $F_n \not\equiv 0 \pmod{p}$. Then, either,

(1)
$$H_n \equiv ((-1 + \sqrt{5})/2)F_n + F_{n+1} \equiv 1 \pmod{p}$$
$$H'_n \equiv ((-1 - \sqrt{5})/2)F_n + F_{n+1} \equiv -1 \pmod{p}$$

or

(2)
$$H_n \equiv ((-1 + \sqrt{5})/2)F_n + F_{n+1} \equiv -1 \pmod{p}$$
$$H'_n \equiv ((-1 - \sqrt{5})/2)F_n + F_{n+1} \equiv 1 \pmod{p}.$$

In both (1) and (2), by adding H_n and H'_n we see that $F_n \equiv 2F_{n+1} \pmod p$. In (1), by subtracting H'_n from H_n, we obtain $F_n \equiv 2/\sqrt{5}$ and thus $F_{n+1} \equiv 1/\sqrt{5} \pmod p$. In (2), we observe that $F_n \equiv -2/\sqrt{5}$ and $F_{n+1} \equiv -1/\sqrt{5} \pmod p$.

Now, if $F_n \equiv 2F_{n+1}$, then

$$F_{n-1} \equiv F_{n+1} - F_n \equiv -F_{n+1} \pmod p.$$

Note that

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

Thus, if $F_n \equiv 2F_{n+1}$, $F_n \not\equiv 0 \pmod p$, then $F_{n-1} + F_{n+1} \equiv 0$ and $F_{2n} \equiv 0 \pmod p$.

It is known that the only possibilities for $\beta(1, 1, p)$ are 1, 2, or 4. If $\beta(1, 1, p) = 4$, then $\alpha(1, 1, p)$ is an odd number. (See [2].) But, then $F_{2n} \equiv 0$, $F_n \not\equiv 0 \pmod p$ can have no solutions since the zeros of $F_n \pmod p$ can only occur at multiples of $\alpha(1, 1, p)$. Thus, $F_n \equiv 2F_{n+1} \pmod p$ is not solvable if $\beta(1, 1, p) = 4$. Thus, if $\beta(1, 1, p) = 4$, all solutions of $H_n \equiv 1$ or $H'_n \equiv 1 \pmod p$ must be generated by $F_n \equiv 0$, $F_{n+1} \equiv 1 \pmod p$, as we have seen before. Thus, the order of the two Fibonacci groups modulo p must both be $\omega(1, 1, p)$ if $p \neq 5$.

If $\beta(1, 1, p) = 2$, then $\alpha(1, 1, p) \equiv 0 \pmod 4$ [2]. But the first solution for H_n or $H'_n \equiv 1$ generated by an $F_n \not\equiv 0 \pmod p$ can only be $n = \frac{1}{2}\alpha(1, 1, p)$, if such a solution exists. This is true since n must equal $\frac{1}{2}k \cdot \alpha(1,1,p)$ for some odd integer k. But both $H_{\mu(1,1,p)}$ and $H'_{\mu(1,1,p)}$ are $\equiv 1 \pmod p$. Thus, n divides

$$\mu(1, 1, p) = 2\alpha(1, 1, p).$$

Hence, $k = 1$ and $n = \frac{1}{2}\alpha(1,1,p)$. But since $\alpha(1, 1, p) \equiv 0 \pmod 4$, $n = \frac{1}{2}\alpha(1, 1, p) \equiv 0 \pmod 2$; and the product of H_n and $H'_n \equiv -1^n \equiv 1 \pmod p$, not -1, a contradiction. Thus, if $\beta(1, 1, p) = 2$, the order of both Fibonacci groups must be $\mu(1, 1, p)$.

The last case occurs if $\beta(1, 1, p) = 1$. Then $\alpha(1, 1, p) \equiv 2 \pmod 4$ [2]. Hence, $n = \frac{1}{2}\alpha(1, 1, p) \equiv 1 \pmod 2$ is the first place where either H_n or H'_n can be $\equiv 1$ and $F_n \not\equiv 0 \pmod p$. Then the product of H_n and

$$H'_n \equiv -1^n \equiv -1 \pmod p.$$

Now, look at the two congruences:

$$F_{2n} = F_{\alpha(1,1,p)} = F_n F_{n-1} + F_n F_{n+1} \equiv 0 \pmod p$$

and

$$F_{2n+1} = F_{\alpha(1,1,p)+1} = F_n^2 + F_{n+1}^2 \equiv 1 \pmod p.$$

Solving for F_n and F_{n+1}, we see that

$$F_n \equiv \pm 2/\sqrt{5} \quad \text{and} \quad F_{n+1} \equiv \tfrac{1}{2}F_n \equiv \pm 1/\sqrt{5} \pmod p,$$

in agreement with earlier results. Thus, if $\beta(1,1,p) = 1$, the period of one Fibonacci group is $\frac{1}{2}\alpha(1,1,p)$ and the period of the other is $\alpha(1,1,p)$.

We have now proved our first lemma.

Lemma 1. If $(5/p) = 0$ or 1, p an odd prime, then the periods of the two Fibonacci groups $\{H_n\}$ and $\{H'_n\}$ modulo p are both $\mu(1,1,p)$ if $\beta(1,1,p) = 2$ or 4 and $p \neq 5$. If $p = 5$, the period of the unique Fibonacci group is 4. If $\beta(1,1,p) = 1$, the period of one Fibonacci group modulo p is $\alpha(1,1,p) = \mu(1,1,p)$, while the period of the other group is $\frac{1}{2}\mu(1,1,p)$.

To generalize this result to other Fibonacci-like groups, it would be helpful if the product of the n^{th} terms of these sequences, $\{M_n\}$ and $\{M'_n\}$, were $\equiv -1^n \pmod p$ as before. The product of the n^{th} terms of the two Fibonacci-like groups is:

$$((a + \sqrt{a^2 + 4b})/2)^n \cdot ((a - \sqrt{a^2 + 4b})/2)^n \equiv (-b)^n \pmod p.$$

This product will be $\equiv -1^n$ if $b = 1$. From now on, in discussing Fibonacci-like groups $\{M_n\}$ and $\{M'_n\}$ modulo p, b will equal 1 and $(a^2 + 4/p)$ will equal 0 or 1.

If $K_0 = c$, $K_1 = d$ are the first terms of a G.F.L.S., then this sequence can be generated from the corresponding P.F.L.S. by the formula: $K_n = (d - ac)J_n + cJ_{n+1}$. Hence, if $b = 1$,

$$M_n \equiv ((a + \sqrt{a^2 + 4})/2)^n \equiv ((-a + \sqrt{a^2 + 4})/2)J_n + J_{n+1} \pmod p$$

and

$$M'_n \equiv ((a - \sqrt{a^2+4})/2)^n \equiv ((-a - \sqrt{a^2+4})/2)J_n + J_{n+1} \pmod{p}.$$

We will next need a few formulas for P.F.L.S. $\{J_n\}$ with a and b unspecified. These formulas are simply generalizations of some familiar Fibonacci identities:

(a) $$J_{n-1}J_{n+1} - J_n^2 = (-1)^n b^{n-1}$$

(b) $$J_{2n} = bJ_nJ_{n-1} + J_nJ_{n+1}$$

(c) $$J_{2n+1} = bJ_n^2 + J_{n+1}^2 \ .$$

These formulas can easily be proven by induction. If $b = 1$, we obtain exactly the same formulas as for the Fibonacci sequence.

The method for finding the periods of Fibonacci-like groups with $b = 1$ is along the same lines as before. $\beta(a,1,p)$ must be either 1, 2, or 4. To prove this let $n = \alpha(a,1,p)$. Then $J_{n-1}J_{n+1} - J_n^2 \equiv -1^n \pmod{p}$. But $J_n \equiv 0 \pmod{p}$ and

$$1 \cdot J_{n-1} = J_{n+1} - aJ_n \equiv J_{n+1} \pmod{p}.$$

Thus, $J_{n+1}^2 \equiv -1^n \pmod{p}$. If n is odd, $J_{n+1}^2 \equiv -1^n \pmod{p}$; $J_{n+1}^4 \equiv 1$ and $\beta(a,1,p) = 4$. (This also shows that no term J_{2n+1} of a P.F.L.S. with $b = 1$ can be divisible by a prime $p \equiv -1 \pmod{4}$ since $(-1/p) = -1$.) If $J_{n+1}^2 \equiv 1$, then $J_n \equiv \pm 1$. If $J_{n+1} \equiv 1$, $\beta(a,1,p) = 1$. If $J_{n+1} \equiv -1 \pmod{p}$, $\beta(a,1,p) = 2$.

Let us now look at the terms of $\{M_n\}$ and $\{M'_n\}$ which are $\equiv 1 \pmod{p}$. As before if $J_n \equiv 0 \pmod{p}$, then J_{n+1} must be $\equiv 1 \pmod{p}$ and both M_n and $M'_n \equiv 1 \pmod{p}$.

If $J_n \not\equiv 0 \pmod{p}$ and both M_n and M'_n are $\equiv 1 \pmod{p}$, then we have: $(\sqrt{a^2+4})J_n \equiv 0 \pmod{p}$ and $a^2 + 4 \equiv 0 \pmod{p}$. But then there is only one Fibonacci-like group $\{M_n\}$ and $M_n \equiv (a/2)^n \pmod{p}$. But $a^2 + 4 \equiv 0 \pmod{p}$. Thus, $a^2/4 \equiv (a/2)^2 \equiv -1 \pmod{p}$. Thus, $a/2$ belongs to the exponent 4 modulo p if $(a^2 + 4/p) = 0$, and the period of such a Fibonacci-like group (mod p) is 4.

Hence, if either M_n or $M'_n \equiv 1$, $J_n \not\equiv 0$ and $a^2 + 4 \not\equiv 0 \pmod{p}$, then one of M_n, $M'_n \equiv 1$ and the other is $\equiv -1 \pmod{p}$. Solving for J_n and J_{n+1}, we see that $J_{n+1} \equiv \frac{1}{2}aJ_n$ and that

$$J_n \equiv \pm 2/\sqrt{a^2+4}, \qquad J_{n+1} \equiv \tfrac{1}{2}aJ_n \equiv \pm a/\sqrt{a^2+4} \ .$$

Also,

$$1 \cdot J_{n-1} \equiv J_{n+1} - aJ_n \equiv \tfrac{1}{2}aJ_n - aJ_n \equiv -\tfrac{1}{2}aJ_n \equiv -J_{n+1} \pmod{p}.$$

Thus, as before, if $a^2 + 4 \not\equiv 0 \pmod{p}$, the first $n \geq 0$ such that M_n or $M'_n \equiv 1 \pmod{p}$ is generated by a $J_n \not\equiv 0 \pmod{p}$, is $n = \frac{1}{2}\alpha(a,1,p)$, if it exists. If $\beta(a,1,p) = 4$, then no such instance can occur since $\alpha(a,1,p)$ is odd. If $\beta(a,1,p) = 4$, then $\mu(a,1,p) \equiv 4 \pmod{8}$, since $\alpha(a,1,p) \equiv 1 \pmod{2}$.

If $\beta(a,1,p) = 2$, then one can solve for J_n and J_{n+1} by the congruences: $J_{2n} \equiv 0 \pmod{p}$, $J_{2n+1} \equiv -1 \pmod{p}$. Substituting back, one finds that the product of M_n and M'_n is $\equiv 1 \pmod{p}$ in contradiction to what we have determined before. This also shows that $\frac{1}{2}\alpha(a,1,p) \equiv 0 \pmod{2}$, $\alpha(a,1,p) \equiv 0 \pmod{4}$, and $\mu(a,1,p) \equiv 0 \pmod{8}$.

If $\beta(a,1,p) = 1$, we solve for J_n and J_{n+1} by the formulas: $J_{2n} \equiv 0 \pmod{p}$, $J_{2n+1} \equiv 1 \pmod{p}$. Solving, we find that

$$J_n \equiv \pm 2/\sqrt{a^2+4}, \qquad J_{n+1} \equiv \tfrac{1}{2}aJ_n \equiv \pm a/\sqrt{a^2+4} \pmod{p},$$

in accordance with our previous results. Note that this further shows that if $\beta(a,1,p) = 1$, then $(a^2 + 4/p) = 1$. Also, if we substitute back to determine M_n and M'_n, we determine that their product $\equiv -1 \pmod{p}$. This shows that $\frac{1}{2}\alpha(a,1,p) \equiv 1 \pmod{2}$ and $\alpha(a,1,p) \equiv 2 \pmod{4}$ if $\beta(a,1,p) = 1$.

Thus, we have now proved our second lemma.

Lemma 2. The periods of the Fibonacci-like groups $\{M_n\}$ and $\{M'_n\}$ modulo p are both $\mu(a,1,p)$ if $\beta(a,1,p) = 2$ or 4 and $(a^2 + 4/p) = 1$. If $(a^2 + 4/p) = 0$, then the period of the single Fibonacci-like group is 4. If $(a^2 + 4/p) = 1$ and $\beta(a,1,p) = 1$, then the period of one Fibonacci-like group is $\frac{1}{2}\mu(a,1,p)$ while the period of the other group is $\mu(a,1,p)$.

The remainder of this paper will be devoted to finding for a given odd prime p all the P.F.L.S. with $0 \leq a < p$, $b = 1$, and $(a^2 + 4/p) = 0$ or 1, and studying the Fibonacci-like groups that they generate.

To find all $0 \leq a < p$ such that $(a^2 + 4/p) = 0$ or 1, all one needs to do is find all solutions of the congruence:

$$x^2 - a^2 = (x + a)(x - a) \equiv 4 \pmod{p}.$$

There are $p - 1$ sets of solutions for x and a, generated by

$$(x + a) \equiv k, \qquad (x - a) \equiv 4/k \pmod{p}, \qquad 1 \leq k \leq p - 1.$$

In general, 4 sets of solutions lead to the same x^2 and a^2:

$$(x + a) \equiv k, \quad (x - a) \equiv 4/k; \qquad (x + a) \equiv 4/k, \quad (x - a) \equiv k;$$

$$(x + a) \equiv -k, \quad (x - a) \equiv -4/k; \qquad (x + a) \equiv -4/k, \quad (x - a) \equiv -k \pmod{p}.$$

Since $k \not\equiv 0$, $k \not\equiv -k$ and $4/k \not\equiv -4/k \pmod{p}$. However, $4/k \equiv k$ iff $k \equiv \pm 2 \pmod{p}$. Also, $-4/k \equiv k$ iff $k \equiv \pm\sqrt{-4} \pmod{p}$. Combining these facts with the fact that p, an odd prime, $\equiv 1 \pmod 4$ iff both ± 4 are quadratic residues modulo p, one finds that the number of solutions of $x^2 \equiv a^2 + 4 \pmod{p}$ is $n + 1$, if $p =$ either $4n + 1$ or $4n + 3$.

I next claim that the set of numbers of the form $(a \pm \sqrt{a^2 + 4})/2$, where $0 \leq a < p$ and $(a^2 + 4/p) = 0$ or 1, gives rise to all the non-zero residues of p. In general, $(a \pm \sqrt{a^2 + 4})/2$ gives rise to two distinct residues, a and $-a$, except in the case where $a \equiv 0 \pmod{p}$. Combining all these conditions with the fact that $a^2 + 4 \equiv 0 \pmod{p}$ is solvable only if $p \equiv 1 \pmod 4$, we see that all the non-zero residues are obtained if the congruences:

$$(a_1 \pm \sqrt{a_1^2 + 4})/2 \equiv (a_2 \pm \sqrt{a_2^2 + 4})/2$$

imply that $a_1 \equiv a_2 \pmod{p}$.

In each of the different cases, if we put the square roots on the same side of the congruence, square both sides and collect terms, we obtain the congruence:

$$4a_1^2 - 8a_1a_2 + 4a_2^2 = 4(a_1 - a_2)^2 \equiv 0 \pmod{p}.$$

Thus, $a_1 \equiv a_2 \pmod{p}$.

Combining our previous results, we are now ready to state our main theorem. The P.F.L.S. with recursion relation: $J_{n+1} = aJ_n + bJ_{n-1}$ will be denoted by $\{J_{a,b}\}$.

Theorem 1. If p is an odd prime equal to either $4n + 1$ or $4n + 3$, then there are $2n + 1$ P.F.L.S. $\{J_{a,1}\}$ with $0 \leq a \leq p - 1$ and $b = 1$, such that $(a^2 + 4/p) = 0$ or 1. These generate $p - 1$ Fibonacci-like groups, the first terms of which are equal to each of the $p - 1$ non-zero residues modulo p.

The exponent e to which a non-zero residue r belongs modulo p is equal to the period of the Fibonacci-like group of which it is the first term.

(1) If $e \equiv 1 \pmod 2$, then $e = \frac{1}{2}\mu(a,1,p)$ for some P.F.L.S. $\{J_{a,1}\}$ with $a < p$ and $\beta(a,1,p) = 1$.

(2) If $e \equiv 2 \pmod 4$, then $e = \mu(a,1,p)$ for some P.F.L.S. $\{J_{a,1}\}$ with $a < p$ and $\beta(a,1,p) = 1$.

(3) If $e \neq 4$, $e \equiv 4 \pmod 8$, then $e = \mu(a,1,p)$ for some P.F.L.S. $\{J_{a,1}\}$ with $a < p$ and $\beta(a,1,p) = 4$.

(4) If $e \equiv 0 \pmod 8$, then $e = \mu(a,1,p)$ for some P.F.L.S. $\{J_{a,1}\}$ with $a < p$ and $\beta(a,1,p) = 2$.

(5) If $e = 4$, then there exist $\phi(4) = 2$ P.F.L.S. $\{J_{a,1}\}$ with $a < p$, $\alpha(a,1,p) = p$, and $\beta(a,1,p) = 4$. Each P.F.L.S. generates a Fibonacci-like group with a period of 4.

This theorem leads to a number of interesting corollaries. Unless stated otherwise, p is an odd prime, $b = 1$, and $(a^2 + 4/p) = 0$ or 1.

Corollary 1. If $0 \leq a \leq p - 1$, and $b = 1$, then the period of any P.F.L.S., $\{J_{a,1}\}$, divides $p - 1$, is even, and is not equal to 4. If d divides $p - 1$ and $d \equiv 2 \pmod 4$, then the number of P.F.L.S. $\{J_{a,1}\}$, $a < p$, with $\mu(a,1,p) = d$ is $\phi(d)$. If $d \neq 4$ and $d \equiv 0 \pmod 4$, then the number of P.F.L.S. $\{J_{a,1}\}$, $a < p$, with $\mu(a,1,p) = d$ is $\frac{1}{2}\phi(d)$.

Proof. This follows from Theorem 1 and the fact that the number of residues belonging to a particular exponent e modulo p, where e divides $p - 1$, is $\phi(e)$.

The next corollary is very important. It states that for any odd prime, p, there exist an infinite number of P.F.L.S. with the maximum possible period modulo p.

Corollary 2. If $0 \leq a < p$, $p \neq 5$, then the number of P.F.L.S. $\{J_{a,1}\}$ with a maximal period of $p - 1$ is

$\frac{1}{2}\phi(p-1)$ if $p-1 \equiv 0 \pmod 4$. If $p-1 \equiv 2 \pmod 4$, then the number of P.F.L.S. $\{J_{a,1}\}$ with a maximal period modulo p of $p-1$ is $\phi(p-1)$. If $p=5$, then the P.F.L.S. $\{J_{1,1}\} = \{F_n\}$ and $\{J_{4,1}\}$ each have periods of 20. (These periods are maximal since $(1^2+4/5) = (4^2+4/5) = 0$ and $\beta(1,1,5) = \beta(4,1,5) = 4$.) If a now ranges over the non-negative integers, then there are an infinite number of P.F.L.S. $\{J_{a,1}\}$ with a maximal period modulo p.

Proof. If $(a^2+4/p) = 1$, then one can generate a Fibonacci-like group whose period is at most $p-1$ and which equals $\mu(a,1,p)$. Thus, $\mu(a,1,p)$ is at most $p-1$. If $a \equiv d \pmod p$, then the P.F.L.S. $\{J_{a,1}\}$ and $\{J_{d,1}\}$ have the same period modulo p. The rest follows from Corollary 1.

If $(a^2+4/p) = -1$, then Corollary 2 does not apply, but we can still find isolated cases of P.F.L.S. $\{J_{a,1}\}$ with maximal periods. If $(a^2+4) = -1$ and $\beta(a,1,p) = 2$ or 4, then $\mu(a,1,p)$ can be at most $2(p+1)$. Examples are: $(5/7) = -1$, $\beta(1,1,7) = 2$ and $\mu(1,1,7) = 16$; and $(5/13) = -1$, $\beta(1,1,13) = 4$, $\mu(1,1,13) = 28$. Note that if $\beta(a,1,p) = 1$, then (a^2+4/p) must = 1 as we have shown earlier, and the maximal period modulo p is $p-1$.

Corollary 3. If $0 \leqslant a < p$ and $p \equiv 3 \pmod 4$, then every P.F.L.S. $\{J_{a,1}\}$ has $\beta(a,1,p) = 1$.

Proof. This follows from the fact that $p-1 \equiv 2 \pmod 4$.

Corollary 4. If $1 \leqslant a < p$, then no P.F.L.S. $\{J_{a,1}\}$ has $\beta(a,1,p) = 1$ iff p is a Fermat prime $= 2^{2^n}+1$. If $a \equiv 0 \pmod p$, then one gets the trivial P.F.L.S. $(0,1,0,1,\cdots)$ with $\beta(a,1,p) = 1$. This gives rise to the 2 trivial Fibonacci-like groups, $\{1^n\}$ and $\{-1^n\}$.

Corollary 5. If $0 \leqslant a < p$ and $p-1 = 2^k \prod_i p_i$, $p_i \equiv 1 \pmod 2$, then the number of P.F.L.S. $\{J_{a,1}\}$ with $\beta(a,1,p) = 1$ is

$$\sum_{d \mid \frac{p-1}{2^k}} \phi(d) = \frac{p-1}{2^k} = \prod_i p_i^{k_i} .$$

The number of P.F.L.S. $\{J_{a,1}\}$ with $\beta(a,1,p) = 2$ is

$$\frac{1}{2} \sum_{\substack{d \mid p-1 \\ d \equiv 0 \pmod 8}} \phi(d) .$$

The number of P.F.L.S. $\{J_{a,1}\}$ with $\beta(a,1,p) = 4$ is

$$\frac{1}{2} \sum_{\substack{d \mid p-1 \\ d \equiv 4 \pmod 8}} \phi(d) .$$

Corollary 6. If $0 \leqslant a < p$ and e is an even number dividing $p-1$, then the summation of all the a's of P.F.L.S. $\{J_{a,1}\}$ with $\mu(a,1,p) = e$ is $\equiv 0 \pmod p$. In addition, the summation of all the a's of P.F.L.S. $\{J_{a,1}\}$ with $\mu(a,1,p)$ dividing e is $\equiv 0 \pmod p$.

Proof. One can prove this by using the fact that if r belongs to the exponent e modulo p, then so does $1/r$. Combine this with the fact that if $r \equiv (a \pm \sqrt{a^2+4})/2 \pmod p$, then $1/r \equiv (-a \pm \sqrt{(-a)^2+4})/2 \pmod p$, and we obtain the result.

One of my purposes in writing this paper was to see if I could get any general results on the relation between residues and the primes of which they were primitive roots. Unfortunately, I was unable to obtain any new results. But I will close this paper with an indication of how one might use P.F.L.S. and Fibonacci-like groups to obtain results about primitive roots. I will prove, using my method, the well-known result that if s and $2s+1$ are primes, $s \equiv 3 \pmod 4$, then all quadratic non-residues are primitive roots modulo $2s+1$, excluding -1.

I will use a result of Robert Backstrom [1], to prove this. He stated that if s is a prime and $p = 2s+1$ is prime such that $(-b/p) = -1$ and $(a^2+4b/p) = +1$, then $\alpha(a,b,p) = p-1$. If $b = 1$, then $p \equiv 3 \pmod 4$, since $(-b/p) = -1$. Hence, $p-1 \equiv 2 \pmod 4$. Thus, every P.F.L.S. $\{J_{a,1}\}$, $0 \leqslant a < p$, $(a^2+4/p) = 1$, has $\beta(a,1,p) = 1$ by

Corollary 3. The only periods that a P.F.L.S. $\{J_{a,1}\}$ can have is 2 or $p-1$, the only even numbers dividing $p-1$. It is easily seen that $\frac{1}{2}(p-3)$ of these P.F.L.S. have a period of $p-1$, each giving rise to one Fibonacci-like group with a period of $\frac{1}{2}(p-1)$ and one with a period of $p-1$. Those with periods of $\frac{1}{2}(p-1)$ correspond to the quadratic residues of p excluding 1, and the others correspond to the quadratic non-residues, excluding -1.

REFERENCES

1. Robert P. Backstrom, "On the Determination of the Zeros of the Fibonacci Sequence," *The Fibonacci Quarterly,* Vol. 4, No. 4 (Dec. 1966), pp. 313–322.
2. John H. Halton, "On the Divisibility Properties of Fibonacci Numbers," *The Fibonacci Quarterly,* Vol. 4, No. 3 (Oct. 1966), pp. 217–240.
3. Lawrence E. Somer, "The Fibonacci Group and a New Proof That $F_{p-(5/p)} \equiv 0 \pmod{p}$," *The Fibonacci Quarterly,* Vol. 10, No. 4 (Oct. 1972), pp. 345–348, 354.

****

SOLUTION OF A CERTAIN RECURRENCE RELATION

DOUGLAS A. FULTS
Student, Saratoga High School, Saratoga, California

At the recent research conference of the Fibonacci Association, Marjorie Bicknell-Johnson gave the recurrence relation

$$P_{r+1} - 2P_r - P_{r-1} + P_{r-2} = 0, \qquad r = 3, 4, \cdots, \tag{1}$$

that represents the number of paths for r reflections in three glass plates (with initial values $P_1 = 1$, $P_2 = 3$ and $P_3 = 6$). I submit here an explicit expression for P_r, and also obtain its generating function.

Based on the usual theory for such relationships, the general solution of (1) can be given in the form

$$P_r = C_1 R_1^r + C_2 R_2^r + C_3 R_3^r, \tag{2}$$

where the quantities R_1, R_2 and R_3 are the roots of the equation

$$R^3 - 2R^2 - R + 1 = 0, \tag{3}$$

and the constants C_1, C_2 and C_3 must be determined to fit the specified conditions.

This cubic, whose discriminant is equal to 49, has three real roots, and they can best be expressed in trigonometric form, as texts on theory of equations seem to say. The roots of (3) are

$$\begin{cases} R_1 = \frac{2}{3}\left[1 + \sqrt{7}\cos\phi\right] \\ R_2 = \frac{1}{3}\left[2 - \sqrt{7}\cos\phi + \sqrt{21}\sin\phi\right] \\ R_3 = \frac{1}{3}\left[2 - \sqrt{7}\cos\phi - \sqrt{21}\sin\phi\right] \end{cases} \tag{4}$$

where

$$\phi = \frac{1}{3}\arccos\left(\frac{1}{2\sqrt{7}}\right). \tag{5}$$

Such roots can be represented exactly only if they are left in this form. (Approximations of them are

$$R_1 = 2.2469796, \qquad R_2 = 0.5549581, \quad \text{and} \quad R_3 = -0.8019377.)$$

The constants in the solution (2) are then found by solving the linear system

[Continued on page 45.]