POSSIBLE PERIODS OF PRIMARY FIBONACCI-LIKE SEQUENCES WITH RESPECT TO A FIXED ODD PRIME

LAWRENCE SOMER
1400 20th St., NW #619, Washington, D.C. 20036

(Submitted February 1981)

1. INTRODUCTION

Let $\{u_n\}$ be a primary Fibonacci-like sequence (PFLS) defined by the recursion relation

$$u_{n+2} = au_{n+1} + bu_n, \tag{1}$$

where $u_0 = 0$, $u_1 = 1$, and a and b are integers. We will call a and b the parameters of the recurrence. We will denote such a sequence as $u(a, b)$. Two of the most important questions concerning these sequences are: For a given PFLS $u(a, b)$, which odd primes have a maximal rank of apparition? and For which odd primes does the PFLS $u(a, b)$ have a maximal period modulo p? No definitive results are known for these questions. What we propose to do in this paper is to first present the best known results concerning these questions. Then we will turn the questions around and fix the odd prime and ask which PFLS's have maximal ranks of apparition and maximal periods with respect to that prime. In a previous paper [6], the author obtained partial results by considering only those PFLS's $u(a, b)$ for which $b = 1$.

Before proceeding further, we will need a few definitions. We will let $\mu(a, b, p)$ denote the period of the PFLS $u(a, b)$ reduced modulo p, where p is an odd prime. Moreover, $\alpha(a, b, p)$ will denote the rank of apparition of p in the PFLS $u(a, b)$. Let $s(a, b, p)$ be the multiplier of the PFLS $u(a, b)$ modulo p. If $k = \alpha(a, b, p)$, then $s(a, b, p) \equiv u_{k+1} \pmod{p}$. Then

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p)$$

is the exponent of the multiplier $s(a, b, p)$ modulo p. Let the characteristic polynomial of the PFLS $u(a, b)$ be

$$x^2 - ax - b = 0. \tag{2}$$

Let $r_1 = (a + \sqrt{a^2 + 4b})/2$ and $r_2 = (a - \sqrt{a^2 + 4b})/2$ be the roots of this polynomial. Then by the Binet equations

$$u_n = (r_1^n - r_2^n)/(r_1 - r_2). \tag{3}$$

Let

$$D = a^2 + 4b = (r_1 - r_2)^2$$

be the discriminant of the characteristic polynomial. Throughout this paper K will denote the algebraic number field $Q(\sqrt{D})$. R will denote the integers of K. Further, Z_p and $\mathrm{GF}(p^2)$ will denote the Galois fields with p and p^2 elements, respectively. Finally, $\mathrm{ord}_p(d)$ will denote the exponent of d modulo p.

2. PRELIMINARY RESULTS

The following well-known results will be necessary for our later theorems.

LEMMA 1: Let p be a prime. In the PFLS $u(a, b)$, *suppose that* $b \not\equiv 0 \pmod{p}$. *Then the* PFLS $u(a, b)$ *is purely periodic modulo p and if* $u \equiv 0 \pmod{p}$, *then*

$$\alpha(a, b, p) \mid k. \tag{4}$$

If $b \equiv 0$ *and* $a \not\equiv 0 \pmod{p}$, *then the rank of apparition of p in* $u(a, b)$ *is undefined and* $u(a, b)$ *reduced modulo p is of the form*

$$(0, 1, a, a^2, a^3, \ldots).$$

If $b \equiv 0$ *and* $a \equiv 0 \pmod{p}$, *then* $u(a, b)$ *reduced modulo p is of the form*

$$(0, 1, 0, 0, 0, \ldots).$$

PROOF: Suppose the pair (u_k, u_{k+1}) is the first pair of consecutive terms to repeat and $k \neq 0$. Let $m = \mu(a, b, p)$. Then $u_{k+m} \equiv u_k$ and $u_{k+1+m} \equiv u_{k+1} \pmod{p}$. However, by the recursion relation (1),

$$bu_{k-1} = u_{k+1} - au_k.$$

Since $b \not\equiv 0 \pmod{p}$,

$$u_{k-1} \equiv (u_{k+1} - au_k)/b \pmod{p}.$$

Thus, the pair (u_{k-1}, u_k) also repeats, which is a contradiction if $k \neq 0$. Thus, the pair (u_0, u_1) repeats. Hence, $u(a, b)$ is purely periodic modulo p. A similar argument shows that if $u_k \equiv 0 \pmod{p}$, then $\alpha(a, b, p) \mid k$. The rest of the lemma follows by direct verification.

LEMMA 2: Let p be an odd prime. In the PFLS $u(a, b)$, *suppose* $b \not\equiv 0 \pmod{p}$. *Then*

$$u_{p-(D/p)} \equiv 0 \pmod{p},$$

where (D/p) is the Legendre symbol for the quadratic character of D modulo p. Further,

$$u_p \equiv (D/p) \pmod{p}.$$

PROOF: See [1, pp. 315-317] or [2, p. 45].

COROLLARY: Let p be an odd prime. Consider the PFLS $u(a, b)$. *Suppose* $b \not\equiv 0 \pmod{p}$. *Then if* $(D/p) = 1$,

$$\alpha(a, b, p) \mid p - 1$$

and $p - 1$ *is the maximal value for* $\alpha(a, b, p)$. *Further, if* $(D/p) = 1$,

$$\mu(a, b, p) \mid p - 1$$

and $p - 1$ *is the maximal value for* $\mu(a, b, p)$. *If* $(D/p) = -1$,

$$\alpha(a, b, p) \mid p + 1$$

and $p + 1$ *is the maximal value for* $\alpha(a, b, p)$. *Moreover, if* $(D/p) = -1$,

$$\mu(a, b, p) \mid p^2 - 1$$

and $p^2 - 1$ *is the maximal value for* $\mu(a, b, p)$.

3. SPECIAL PRIMES HAVING MAXIMAL PERIODS AND RANKS OF APPARITION

We will now see that given specific PFLS's $u(a, b)$, there exists a class of primes dependent on the parameters a and b with maximal ranks of apparition and maximal periods. In the case of ranks of apparition, we will also obtain the next best result, namely half-maximal ranks of apparition. We now present the following results.

LEMMA 3: Let p be an odd prime. Consider the PFLS $u(a, b)$. *Suppose* $p \nmid abD$.

(i) *If* $(-b/p) = 1$, *then*

$$u_{(p-(D/p))/2} \equiv 0 \pmod{p}.$$

(ii) *If* $(-b/p) = -1$, *then*

$$u_{(p-(D/p))/2} \not\equiv 0 \pmod{p}.$$

PROOF: See D. H. Lehmer [5] or Robert P. Backstrom [1].

THEOREM 1: Let p be an odd prime. Consider the PFLS $u(a, b)$. *Suppose* $p \nmid abD$.

(i) *If r is a prime and $p = 2r + 1$ is a prime such that* $(-b/p) = (D/p) = 1$, *then*

$$\alpha(a, b, p) = r = (p - 1)/2.$$

(ii) *If s is a prime and $p = 2s - 1$ is a prime such that $(-b/p) = (D/p) = -1$, then*

$$\alpha(a, b, p) = p + 1.$$

(iii) *If s is a prime and $p = 2s - 1$ is a prime such that $(-b/p) = 1$ and $(D/p) = -1$, then*

$$\alpha(a, b, p) = s = (p + 1)/2.$$

(iv) *If r is a prime and $p = 2r + 1$ is a prime such that $(-b/p) = -1$ and $(D/p) = 1$, then*

$$\alpha(a, b, p) = p - 1.$$

PROOF: See Backstrom [1]. This proof relies heavily on Lemma 3.

COROLLARY: Let p be an odd prime. Consider the PFLS $u(a, b)$. *Suppose $p \nmid abD$.*

(i) *If r is a prime and $p = 2r + 1$ is a prime such that $(-b/p) = (D/p) = 1$,*

$$\mu(a, b, p) = p - 1.$$

(ii) *If s is a prime and $p = 2s - 1$ is a prime such that $(D/p) = 1$ and $-b$ is a primitive root* modulo p, *then*

$$\mu(a, b, p) = p^2 - 1.$$

PROOF: (i) By the corollary to Lemma 2, $\mu(a, b, p)$ is at most $p - 1$ and the result now follows.

(ii) By Lemma 2,

$$u_p \equiv (D/p) \equiv -1 \pmod{p}$$

and

$$u_{p-(D/p)} = u_{p+1} \equiv 0 \pmod{p}.$$

Now, by the recursion relation,

$$s(a, b, p) = u_{\alpha(a,b,p)+1} = u_{p+2} = bu_p + au_{p+1}$$
$$\equiv -b + 0 \equiv -b \pmod{p}.$$

Further,

$$\text{ord}_p(s(a, b, p)) = \text{ord}_p(-b) = p - 1$$

by hypothesis. Thus,

$$\begin{aligned}\mu(a,\ b,\ p) &= \ (a,\ b,\ p) \cdot \operatorname{ord}_p(s(a,\ b,\ p)) \\ &= (p + 1)(p - 1) = p^2 - 1.\end{aligned}$$

Unfortunately, it is not known if there exist an infinite number of pairs of primes of the form $(r,\ 2r + 1)$ or $(s,\ 2s - 1)$. Two other classic sets of primes, the Mersenne primes, $M_q = 2^q - 1$, where q is a prime, and the Fermat primes, $F_n = 2^{2^n} + 1$, can have maximal periods. We have the following theorems.

THEOREM 2: Consider the PFLS $u(a,\ b)$. *Let* $p = M_q = 2^q - 1$ *be a Mersenne prime.*

(i) *If* $(-b/p) = (D/p) = -1$, *then*

$$\alpha(a,\ b,\ p) = p + 1.$$

(ii) *If* $(D/p) = -1$ *and* $-b$ *is a primitive root* modulo p, *then*

$$\mu(a,\ b,\ p) = p^2 - 1.$$

PROOF: (i) By Lemma 2, $u_{p+1} \equiv 0 \pmod{p}$. Now by Lemma 1, if $u_k \equiv 0 \pmod{p}$, then $\alpha(a,\ b,\ p) \mid k$. Moreover, by Lemma 3, $p \nmid u_{(p+1)/2}$. The only divisors of $p + 1$ are 2^n, where $0 \leqslant n \leqslant q$. Thus,

$$\alpha(a,\ b,\ p) = p + 1,$$

since this is the only divisor of $p + 1$ not dividing $(p + 1)/2$.

(ii) This follows from the same argument used in the proof of assertion (ii) of the corollary to Theorem 1.

THEOREM 3: Consider the PFLS $u(a,b)$. *Let* $p = F_n = 2^{2^n} + 1$ *be a Fermat prime. If* $(-b/p) = -1$ *and* $(D/p) = 1$, *then*

$$\alpha(a,\ b,\ p) = \mu(a,\ b,\ p) = p - 1.$$

PROOF: By Lemma 2 and its corollary, $\alpha(a,\ b,\ p) \mid p_n - 1$ and $\mu(a,\ b,\ p) \mid p - 1$. The only divisors of $p - 1$ are 2^k, where $0 \leqslant k \leqslant 2$. But by Lemma 3, we have $p \nmid u_{(p-1)/2}$. Therefore,

$$\alpha(a,\ b,\ p) = \mu(a,\ b,\ p) = p - 1,$$

since this is the only divisor of $p - 1$ not dividing $(p - 1)/2$.

Unfortunately, again, it is not known if there are an infinite number of Mersenne or Fermat primes.

4. PRELIMINARY LEMMAS FOR THE GENERAL CASE

Theorems 1, 2, and 3 and the corollary to Theorem 1 are limited in that, for a specific PFLS, we do not know if there are an infinite number of primes having the required form to assure that these primes have maximal ranks of apparition or periods. What we intend to do is, instead of fixing the PFLS $u(a, b)$, we will fix the prime and ask if there are PFLS's for which the rank of apparition or period is a maximum. The answer is "yes" for both the cases $(D/p) = 1$ and $(D/p) = -1$, and there are an infinite number of PFLS's which satisfy this condition. More generally, given an odd prime p, we will vary over all PFLS's and investigate the possible values for the period, rank of apparition, exponent of the multiplier, and multiplier modulo p. In the first three cases, we shall see that there exist PFLS's reduced modulo p for which the function takes on a maximal value. Clearly, if we let the parameters a and b vary over all the integers rather than just the integers between 0 and $p - 1$, we will obtain an infinite number of PFLS's $u(a, b)$ with this property. We will now need the following four lemmas.

__LEMMA 4__: Let p be an odd prime. Suppose that $p \nmid bD$. Let P be a prime ideal in $K = Q(\sqrt{D})$ dividing p. Consider the PFLS *$u(a, b)$.*

(i) *$\mu(a, b, p)$ is the least common multiple of the exponents of r_1 and r_2* modulo *P.*

(ii) *$\alpha(a, b, p)$ is the exponent of r_1/r_2* modulo *P. This is also the least positive integer n such that $r_1^n \equiv r_2^n$* (mod *P). If $(D/p) = -1$, then $\alpha(a, b, p)$ is also the least positive integer n such that r_1^n is congruent to a rational integer* modulo *P.*

(iii) *If $k = \alpha(a, b, p)$, then*

$$s(a, b, p) \equiv r_1^k \pmod{P}.$$

PROOF: Let R denote the integers of K. Since $b \not\equiv 0 \pmod{p}$, neither r_1 nor $r_2 \equiv 0 \pmod{P}$. Since R/P is a field of p or p^2 elements, $r_1/r_2 \pmod{P}$ is well-defined.

(i) Let $n = \mu(a, b, p)$. Then

$$u_n \equiv 0 \pmod{p} \equiv 0 \pmod{P}$$

and

$$u_{n+1} \equiv 1 \pmod{p} \equiv 1 \pmod{P}$$

by definition of $\mu(a, b, p)$. Since $D = (r_1 - r_2)^2 \not\equiv 0 \pmod{p}$,

$$u_n = (r_1^n - r_2^n)/(r_1 - r_2)$$

is well-defined modulo P. Since

$$(r_1^n - r_2^n)/(r_1 - r_2) \equiv 0 \pmod{P},\ r_1^n \equiv r_2^n \pmod{P}.$$

Hence,

$$u_{n+1} \equiv (r_1^n(r_1) - r_1^n(r_2))/(r_1 - r_2) \equiv r_1^n \equiv 1 \pmod{P}.$$

Thus,

$$r_1^n \equiv r_2^n \equiv 1 \pmod{P}.$$

Conversely, if

$$r_1^k \equiv r_2^k \equiv 1 \pmod{P},$$

then it easily follows that $u_k \equiv 0 \pmod{p}$ and $u_{k+1} \equiv 1 \pmod{p}$. Assertion (i) now follows.

(ii) Now let $n = \alpha(a, b, p)$. Then

$$u_n = (r_1^n - r_2^n)/(r_1 - r_2) \equiv 0 \pmod{P}.$$

This occurs only if $r_1^n \equiv r_2^n \pmod{P}$. Dividing through by r_2^n, we obtain

$$(r_1/r_2)^n \equiv 1 \pmod{P},$$

and hence $\alpha(a, b, p)$ is the exponent of $r_1/r_2 \pmod{P}$. Further, if $(D/p) = -1$, let σ be the automorphism of the Galois field R/P of p^2 elements. Then

$$\sigma(r_1) = r_1^p \equiv r_2 \pmod{P}$$

and

$$\sigma(r_1^n) = (r_1^p)^n \equiv r_2^n \pmod{P}.$$

Thus, if $r_1^n \equiv r_2^n \pmod{P}$, we obtain $(r_1^n)^p \equiv r_1^n \pmod{P}$. Now, $R/P = Z_p[\sqrt{D}]$, where Z_p is the field with p elements. In $Z_p[\sqrt{D}]$, the only solutions of the equation

$$x^p - x = 0$$

are those in Z_p by Fermat's theorem. Consequently, the rest of assertion (ii) now follows.

(iii) Let $k = \alpha(a, b, p)$. Then

$$u_{k+1} \equiv s(a, b, p) \pmod{p} \equiv s(a, b, p) \pmod{P}.$$

By the proof of (ii), $r_1^k \equiv r_2^k \pmod{P}$. Thus,

$$u_{k+1} = (r_1^{k+1} - r_2^{k+1})/(r_1 - r_2) \equiv (r_1^k(r_1) - r_1^k(r_2))/(r_1 - r_2)$$

$$\equiv r_1^k \equiv s(a, b, p) \pmod{P}.$$

The proof is now complete.

LEMMA 5: Let p be an odd prime. Let m be a residue modulo p. *Then, given a fixed integer a, there exists a unique residue b* (mod p) *such that in the* PFLS $u(a, b)$, $(D/p) = 0$ *or* 1 *and* $r_1 \equiv m$ (mod p).

PROOF: We want

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

Then

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

Solving for b, we see that $b \equiv m^2 - am$ (mod p) suffices. Note that if $m \equiv a/2$ (mod p), then $r_1 \equiv r_2$ (mod p) and $(D/p) = 0$.

LEMMA 6: Let $m \not\equiv 0$ (mod p) *be some residue* modulo p, *where p is an odd prime. Then, given a fixed integer b, where $b \not\equiv 0$* (mod p), *there exists a unique residue a* (mod p) *such that in the* PFLS $u(a, b)$, $(D/p) = 0$ *or* 1 *and* $r_1 \equiv m$ (mod p).

PROOF: By the proof of Lemma 5, if such a residue a exists,

$$b \equiv m^2 - am \pmod{p}.$$

Solving for a, we obtain

$$a \equiv (m^2 - b)/m \pmod{p}.$$

Thus, such a residue a does exist. Note that if $m^2 \equiv -b$ (mod p), then

$$r_2 \equiv -b/m \equiv m \equiv r_1 \pmod{p}$$

and $(D/p) = 0$.

LEMMA 7: Let m and n be a fixed pair of residues modulo p *where p is an odd prime. Then there exists a unique* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 0$ *or* 1 *and* $r_1 \equiv m$, $r_2 \equiv n$ (mod p).

PROOF: Suppose that such a PFLS $u(a, b)$ does exist. Then $r_1 \equiv m$ and $r_2 \equiv n$ (mod p). Further, $r_1 + r_2 = a$. Moreover, $r_1 r_2 = -b$. Thus,

$$a \equiv m + n,\ b \equiv -mn \pmod{p}$$

suffice as the parameters of the PFLS $u(a, b)$. Note that if $m \equiv n$ (mod p), then $r_1 \equiv r_2$ (mod p) and $(D/p) = 0$.

5. THE CASE $(D/p) = 1$

We are now ready to present our main results.

THEOREM 4: *Let p be an odd prime and let $d \neq 1$ be a divisor of $p - 1$. Let $t(d)$ be the number of ways of expressing d as the least common multiple of the exponents of the nonzero residues m and n* (mod p), *where* $m \not\equiv n$ (mod p). *Then there exist* $t(d)$ PFLS's $u(a, b)$, *where* $0 \leqslant a \leqslant p - 1$ *and* $1 \leqslant b \leqslant p - 1$, *reduced* modulo p, *such that* $(D/p) = 1$ *and* $\mu(a, b, p) = d$. *In particular there exist* $t(p - 1)$ *reduced* PFLS's $u(a, b)$ *with a maximal period of* $p - 1$.

PROOF: First, by the corollary to Lemma 2, $\mu(a, b, p)$ is at most $p - 1$. By Lemma 4(i), $\mu(a, b, p)$ is the least common multiple of the exponents of r_1 and r_2 modulo p. By Lemma 7, for any pair of residues m and n, where $m \not\equiv n$ (mod p), we can find a PFLS $u(a, b)$ such that $r_1 \equiv m$ (mod p), $r_2 \equiv n$ (mod p), and $(D/p) = 1$. Since for any positive divisor d of $p - 1$ there exists a residue m such that $\text{ord}_p(m) = d$, the theorem follows.

THEOREM 5: *Let p be an odd prime and let $d \neq 1$ be any positive divisor of $p - 1$. Then there exist exactly* $(p - 1)/2 \cdot \phi(d)$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $b \not\equiv 0$ (mod p), $(D/p) = 1$, *and* $\alpha(a, b, p) = d$. *In particular there exist* $(p - 1)/2 \cdot \phi(p - 1)$ *such* PFLS's *with a maximal rank of apparition of* $p - 1$.

PROOF: $\alpha(a, b, p) = d$ if and only if

$$u_d = (r_1^d - r_2^d)/(r_1 - r_2) \equiv 0 \pmod{p}$$

and $u_n \not\equiv 0$ (mod p) for any positive integer $n < d$. Let $r_2 \equiv gr_1$, where $g \not\equiv 1$ (mod p). Then $r_2^d \equiv g^d r_1^d$. Hence, $\alpha(a, b, p) = d$ if and only if g belongs to the exponent d modulo p. Note that neither r_1 nor $r_2 \equiv 0$ (mod p), since $b \not\equiv 0$ (mod p). Now there exist $\phi(d)$ residues belonging to the exponent d modulo p. Since r_1 can be any one of the $p - 1$ nonzero residues by Lemma 7, we have $(p - 1) \cdot \phi(d)$ ordered pairs of residues, $(r_1, r_2) \equiv (r_1, gr_1)$, such that the corresponding PFLS $u(a, b)$ has a rank of apparition of p equal to d.

We are really interested in the unordered pairs of solutions for r_1 and r_2, since r_1 and r_2 considered in any order determine the same PFLS. The ordered pairs (r_1, r_2) and (r_2, r_1) are equal as unordered pairs. Now, if $r_2 \equiv gr_1$, then $r_1 \equiv r_2/g$, where $g \not\equiv 0$ (mod p), since neither r_1 nor $r_2 \equiv 0$ (mod p). But if g belongs to the exponent d, so does $1/g$. Further, $r_1 \not\equiv r_2$ (mod p), since $(D/p) \neq 0$. Thus, exactly half of the $(p - 1) \cdot \phi(d)$ ordered pairs are equal as unordered pairs. The theorem now follows.

THEOREM 6: *Let p be an odd prime. If $d | p - 1$ and $d \neq p - 1$, then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $b \not\equiv 0$ (mod p), $(D/p) = 1$, *and* $\beta(a, b, p) = d$. *Further, if $s \not\equiv 0$* (mod p) *is a fixed integer, then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $s(a, b, p) \equiv s$ (mod p).

PROOF: By Lemma 7, simply pick residues r_1 and r_2 modulo p such that

$$\text{ord}_p(r_1) = p - 1 \quad \text{and} \quad r_2 \equiv gr_1 \pmod{p},$$

where $\text{ord}_p(g) = (p - 1)/d$ and $g \not\equiv 1 \pmod{p}$. Hence, for the corresponding PFLS $u(a, b)$,

$$\mu(a, b, p) = [\text{ord}_p(r_1), \text{ord}_p(r_2)] = p - 1$$

by Lemma 4(i), where $[m, n]$ is the least common multiple of m and n. By the proof of Theorem 5,

$$\alpha(a, b, p) = (p - 1)/d.$$

Then

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = d.$$

Now suppose that s is a fixed integer and the exponent of s modulo p is d. Then, by elementary number theory, there is a primitive root r_1 of p such that $r_1^{(p-1)/d} \equiv s \pmod{p}$. By the above proof, we can find an integer r_2 such that r_1 and r_2 are the characteristic roots of the PFLS $u(a, b)$ with

$$\mu(a, b, p) = p - 1 \quad \text{and} \quad \alpha(a, b, p) = (p - 1)/d = k.$$

Then

$$s(a, b, p) \equiv r^k \equiv s \pmod{p}$$

and we are done.

6. THE CASE $(D/p) = -1$

Theorems 7, 8, and 9 below will deal with those PFLS's $u(a, b)$ for which $(D/p) = -1$.

THEOREM 7: Let p *be an odd prime. Suppose that* $d|p^2 - 1$ *but* $d \nmid p - 1$. *Then there exist exactly* $(1/2)\phi(d)$ *PFLS's* $u(a, b)$ *reduced* modulo p *such that*

$$(D/p) = -1 \quad \text{and} \quad \mu(a, b, p) = d.$$

In particular, there exist exactly $(1/2)\phi(p^2 - 1)$ *reduced* PFLS's $u(a, b)$ *with a maximal period of* $p^2 - 1$.

PROOF: Look at $\text{GF}(p^2)$, the finite field of p^2 elements. Since the nonzero elements form a cyclic multiplicative group, there exist exactly $\phi(d)$ elements in this field belonging to the exponent d. Let r_1 be one of these elements. Let Z_p represent the field of p elements. Now, $r_1 \in \text{GF}(p^2)$ but $r_1 \notin Z_p$ by Fermat's Little Theorem, since the exponent of r_1 does not divide $p - 1$. So $Z_p[r_1] = \text{GF}(p^2)$. Thus, r_1 satisifes an irreducible polynomial of degree 2 over Z_p:

$$x^2 - ax - b = 0, \tag{5}$$

where $0 \leqslant a \leqslant p - 1$ and $1 \leqslant b \leqslant p - 1$. The other root of this polynomial is $\sigma(r_1) = r_1^p = r_2$. Then

$$r_1 = (a + \sqrt{a^2 + 4b})/2 \quad \text{and} \quad r_2 = (a - \sqrt{a^2 + 4b})/2$$

can be considered elements of $K = Q(\sqrt{a^2 + 4b})$. Let P denote a prime ideal of K dividing p. By assumption, both r_1 and r_2 belong to the exponent d in the field R/P of p^2 elements, since r_1 does and r_2 is automorphic to r_1. Hence, by Lemma 4(i), $\mu(a, b, p) = d$. Finally, it is clear that there exist exactly $(1/2)\phi(d)$ such PFLS's reduced modulo p, since each PFLS $u(a, b)$ is determined by r_1 and r_2.

THEOREM 8: Let p be an odd prime. Suppose $d|p + 1$ and $d \neq 1$. Then, there exist PFLS's *reduced* modulo p, *such that* $(D/p) = -1$ *and* $\alpha(a, b, p) = d$. *In particular, there exist* PFLS's $u(a, b)$ *with a maximal rank of apparition of* p *of* $p + 1$.

PROOF: First, find an element r_1 of GF(p^2) such that r_1 belongs to the exponent $(p - 1)d$. Then r_1 is not a $(p - 1)$st root of unity and, hence, r_1 is not a member of the prime field Z_p. Thus, GF$(p^2) = Z_p[r_1]$. As in the proof of Theorem 7, we can consider r_1 an element of K. Let P be a prime ideal in K dividing p. Then

$$r_1^{(p-1)d} \equiv 1 \pmod{P}$$

and r_1^d is a $(p - 1)$st root of unity in R/P. Hence,

$$r_1^d \equiv z \pmod{P},$$

where z is a rational integer and $z \not\equiv 0 \pmod{p}$, since these are the only residue classes (mod P) that are $(p - 1)$st roots of unity.

Now, suppose that $r_1^n \equiv z' \pmod{p}$, where $0 < n < d$ and z' is a rational integer. Then

$$r_1^{n(p-1)} \equiv 1 \pmod{P}$$

and $n(p - 1) < (p - 1)d$. But this is a contradiction. Thus, d is the least positive integer such that $r_1^d \equiv z \pmod{P}$, where z is a rational integer. Hence, by Lemma 4(ii), $\alpha(a, b, p) = d$.

THEOREM 9: Let p be an odd prime; also let $d|p - 1$. If p is not a Mersenne prime, then there exists a PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = -1$ *and* $\beta(a, b, p) = d$. *If p is a Mersenne prime then there exists at least one* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = -1$ *and* $\beta(a, b, p) = d$ *if and only if d is even. In any case, there exists a* PFLS $u(a, b)$ *with a maximal exponent of the multiplier* modulo p *of* $p - 1$. *Further, if* $d|p - 1$ *and there exists a* PFLS $u(a, b)$ *such that* $\beta(a, b, p) = d$ *and s is any integer whose exponent* modulo p *is d, then there exists a* PFLS $u(a, b)$ *such that* $s(a, b, p) \equiv s \pmod{p}$.

PROOF: Suppose that the period modulo p of a PFLS $u(a, b)$ is k, where

$$k \nmid p - 1,\ k|p^2 - 1, \text{ and } (D/p) = -1.$$

By the proof of Theorem 8, both r_1 and r_2 belong to the exponent k modulo P. It is clear that we can express k uniquely as the product of m and n, where m and n are positive integers, $m|p - 1$, $n|p + 1$, $n > 1$, and $(mn, p - 1) = m$. We shall show that $n = \alpha(a, b, p)$ and $m = \beta(a, b, p)$.

By Lemma 4(ii), $\alpha(a, b, p)$ is the least positive integer c such that r_1^c is congruent to a rational integer modulo P. Now, n is such an integer, because r_1^n is an mth root of 1 in R/P and $m|p - 1$. I claim that no smaller positive integer j suffices. If this were true, then

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = mn/j$$

and mn/j must divide $p - 1$. Clearly,

$$mn/j\,|\,mn$$

also. But, since $j < n$, $mn/j > m$. However, m is the largest integer dividing both m and $p - 1$, so we have a contradiction. Thus, $\alpha(a, b, p) = n$ and $\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = m$.

Now suppose that p is not a Mersenne prime. Clearly, $(p - 1, p + 1) = 2$. Since p is not a Mersenne prime, $p + 1$ has a prime factor $h > 2$ such that $(h, p - 1) = 1$. Let r_1 be any integer in R whose exponent (mod P) is dh. By the proof of Theorem 7, we can find a PFLS $u(a, b)$ such that $(D/p) = -1$, the characteristic roots r_1 and r_2 have exponent dh (mod P), and $\mu(a, b, p) = dh$. It is apparent that $(dh, p - 1) = d$. By our above arguments in this proof, $\beta(a, b, p) = d$. Furthermore, among the $\phi(dh)$, such possibilities for r_1, r_1^h must be one of the $\phi(d)$ residues (mod P) whose expopent is d. Since $(d, h) = 1$, $\phi(dh) = \phi(d)\phi(h)$. Thus, it follows that for any fixed integer s with exponent d (mod p), there exist $\phi(h)$ residues r_1 (mod P) such that $r_1^h \equiv s$ (mod P). Then r_1 and $\sigma(r_1) = r_2$ are the characteristic roots of a unique PFLS $u(a, b)$ modulo p, where σ is the Frobenius automorphism of R/P. By Lemma 4-(iii),

$$r_1^h \equiv s(a, b, p) \equiv s \pmod{p}.$$

Now assume that p is a Mersenne prime. Then $p + 1$ is a power of 2 and $2|p - 1$ but $4\nmid p - 1$. If d is an even number, then by Theorem 7 we can find a PFLS $u(a, b)$ such that $(D/p) = -1$ and $\mu(a, b, p) = 2d$. It is easily seen that $(2d, p - 1) = d$. By our above arguments, $\beta(a, b, p) = d$. Further, by using our arguments above, if s is a residue (mod p) whose exponent is d, then there exists a PFLS $u(a, b)$ such that $s(a, b, p) \equiv s$ (mod p). If d is an odd number, it is impossible to find positive integers h and k such that $dh = k$, $d|p - 1$, $h|p + 1$, $h > 1$, and $(dh, p - 1) = d$. This is so because h must be a power of 2 greater than 1 and thus $(dh, p - 1) = 2d$, not d. The theorem now follows.

7. THE CASE $(D/p) = 0$

Theorem 10 will explore the case in which $(D/p) = 0$. But first, we will need Lemma 8, which discusses the possibilities for $\mu(a, b, p)$, $\alpha(a, b, p)$, $\beta(a, b, p)$, and $s(a, b, p)$ for such PFLS's $u(a, b)$.

<u>*LEMMA 8:*</u> *In the* PFLS $u(a, b)$, *suppose* $p \nmid ab$, *but* $p \mid D$. *Let* $a' = a/2$. *Then*

$$\alpha(a, b, p) = p,$$
$$\mu(a, b, p) = p \cdot \text{ord}_p(a'),$$
$$s(a, b, p) \equiv a' \pmod{p},$$

and

$$\beta(a, b, p) = \text{ord}_p(a').$$

<u>*PROOF:*</u> The fact that $\alpha(a, b, p) = p$ follows from Lemma 2. The rest of the theorem follows from definition of the terms and the fact that

$$s(a, b, p) \equiv r_1^p \equiv (a/2)^p \equiv (a/2) \pmod{p}.$$

<u>*THEOREM 10:*</u> *Let* p *be an odd prime.*

(i) *There exist exactly* $p - 1$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 0$, $b \not\equiv 0 \pmod{p}$, *and* $\alpha(a, b, p) = p$.

(ii) *If* $d \mid p - 1$, *then there exist exactly* $\phi(d)$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $\beta(a, b, p) = d$ *and* $\mu(a, b, p) = dp$. *If* s *is any integer such that the exponent of* $s \pmod{p}$ *is* d, *then there exists exactly one of these* $\phi(d)$ PFLS's $u(a, b)$ *reduced* modulo p *such that* $s(a, b, p) \equiv s \pmod{p}$.

<u>*PROOF:*</u> (i) $\alpha(a, b, p) = p$ if and only if $a^2 + 4b \equiv 0 \pmod{p}$. Given a nonzero residue a, there is a unique nonzero residue b such that $a^2 + 4b \equiv 0 \pmod{p}$. Assertion (i) now easily follows from Lemma 8 and Lemma 7.

(ii) By Lemma 8, $s(a, b, p) \equiv a/2 \pmod{p}$. The result now easily follows from Lemma 7.

<u>8. THE CASE FOR WHICH b IS A FIXED INTEGER</u>

By Lemma 3, one might suspect that the parameter b might play a large part in determining the divisibility properties of the PFLS $u(a, b)$. The following two well-known identities add further credence to this suspicion, since they depend only on the parameter b.

$$u_n^2 - u_{n-1}u_{n+1} = (-b)^{n-1}. \tag{6}$$

$$u_{m+n} = bu_m u_{n-1} + u_n u_{m+1}. \tag{7}$$

Both (6) and (7) can be proved from the Binet formulas or by induction. So, given a fixed value of b, we should be able to develop some conclusions concerning the possible periods and ranks of apparition of PFLS's $u(a, b)$ with respect to a given odd prime p. In particular, we have the following three theorems.

<u>*THEOREM 11:*</u> *Suppose that p is an odd prime and b is any integer such that $b \not\equiv 0 \pmod{p}$. If $\mu(a, b, p) = d$, then $\text{ord}_p(-b) \mid d$ for any* PFLS *$u(a, b)$ such that $(D/p) = 1$. Let $d \neq 1$ be any integer such that $d \mid p - 1$ and $\text{ord}_p(-b) \mid d$. Further, suppose that it is not the case that both $b \equiv 1 \pmod{p}$ and $d = 4$ or both $b \equiv -1 \pmod{p}$ and $d = 2$. Then there exists at least one* PFLS *$u(a, b)$ reduced* modulo *p such that $\mu(a, b, p) = d$ and $(D/p) = 1$. If $b \equiv 1 \pmod{p}$ and $d = 4$ or $b \equiv -1 \pmod{p}$ and $d = 2$, then no such* PFLS *$u(a, b)$ exists. In particular, if $\text{ord}_p(-b) = p - 1$, then there exists at least one* PFLS *$u(a, b)$ with a maximal period* modulo *p.*

<u>*PROOF:*</u> Firstly, we shall show that if $u(a, b)$ is a PFLS such that $(D/p) = 1$ and $\mu(a, b, p) = d$, then $\text{ord}_p(-b) \mid d$. Note that $-b = r_1 r_2$ and $d = [\text{ord}_p(r_1), \text{ord}_p(r_2)]$ by Lemma 4(i). Thus, it follows that

$$(-b)^d = r_1^d r_2^d \equiv 1 \cdot 1 \equiv 1 \pmod{p}.$$

Thus, $\text{ord}_p(-b) \mid d$. Next, note that if $(D/p) = 1$, then $r_1 \not\equiv r_2 \pmod{p}$. Since $r_2 = -b/r_1$, $r_1 \equiv r_2 \pmod{p}$ if and only if $r_1^2 \equiv -b \pmod{p}$.

If $d \neq 2, 3, 4$, or 6, then $\phi(d) \geqslant 4$. Consequently, we can then choose a residue r_1 modulo p such that $\text{ord}_p(r_1) = d$ and $r_1^2 \not\equiv -b \pmod{p}$, since there are $\phi(d)$ residues $n \pmod{p}$ such that $\text{ord}_p(n) = d$ and at most two residues $m \pmod{p}$ such that $m^2 \equiv -b \pmod{p}$. Then

$$r_2^d \equiv (-b/r_1)^d \equiv 1 \pmod{p},$$

since $\text{ord}_p(-b) \mid d$. Hence, $\text{ord}_p(r_2) \mid \text{ord}_p(r_1)$ and

$$[\text{ord}_p(r_1), \text{ord}_p(r_2)] = d.$$

By Lemma 4(i), $\mu(a, b, p) = d$ for the PFLS $u(a, b)$ corresponding to r_1 and $r_2 \pmod{p}$. By Lemma 6, we can find a PFLS $u(a, b)$ such that its characteristic root r_1 indeed satisfies the conditions that $\text{ord}_p(r_1) = d$ and $r_1^2 \not\equiv -b \pmod{p}$.

Now suppose that $d = 2, 3, 4$, or 6 and we can choose a residue $r_1 \pmod{p}$ such that $\text{ord}_p(r_1) = d$ and $r_1^2 \not\equiv -b \pmod{p}$. Then, by our previous argument, $\mu(a, b, p) = d$.

If $d = 2$ and $r_1^2 \equiv -b \pmod{p}$ for all choices of r_1 such that $\text{ord}_p(r_1) = 2$, then $-b \equiv 1 \pmod{p}$. However, this case is excluded by hypothesis.

If $d = 3$ and $r_1^2 \equiv -b \pmod{p}$ for all choices of r_1 such that $\text{ord}_p(r_1) = 3$, then $\text{ord}_p(-b) = 3$. Now, choose $r_1 \equiv 1 \pmod{p}$. Then

$$r_2 \equiv -b/r_1 \equiv -b \pmod{p}.$$

By Lemma 4(i), $\mu(a, b, p) = 3$.

If $d = 4$ and $r_1^2 \equiv -b \pmod{p}$ for all choices of r_1 such that $\text{ord}_p(r_1) = 4$, then $-b \equiv -1 \pmod{p}$. But this case is excluded by hypothesis.

If $d = 6$ and $r_1 \equiv -b \pmod{p}$ for all choices of r_1 such that $\text{ord}_p(r_1) = 6$, then $\text{ord}_p(-b) = 3$. In this case, choose $r_1 \equiv -1 \pmod{p}$. Then $r_2 \equiv -b/-1 \equiv b \pmod{p}$. Clearly then, $\text{ord}_p(b) = 6$. By Lemma 4(i), $\mu(a, b, p) = 6$.

Now suppose that $b \equiv 1 \pmod{p}$ and $d = 4$. Then $\{u_n\}$ modulo p is of the form

$$u_0 \equiv 0,\ u_1 \equiv 1,\ u_2 \equiv a,\ u_3 \equiv a^2 + 1,$$
$$u_4 \equiv a^3 + 2a \equiv 0,\ u_5 \equiv a^2 + 1,\ \ldots .$$

Since $a^2 + 1 \equiv 1 \pmod{p}$, then $a \equiv 0 \pmod{p}$. But then, $\mu(a, b, p) = 2$ and not 4. Thus, $\mu(a, 1, p)$ can never be 4.

If $b \equiv -1 \pmod{p}$ and $d = 2$, then $\{u_n\}$ modulo p is of the form

$$u_0 \equiv 0,\ u_1 \equiv 1,\ u_2 \equiv 0,\ u_3 \equiv -u_1 \equiv 1,\ \ldots .$$

But it is clearly impossible for u_3 to be both congruent to -1 and 1 if p is an odd prime. Thus, $\mu(a, -1, p)$ never equals 2.

THEOREM 12: Let p be an odd prime, and let b be any integer such that $b \not\equiv 0 \pmod{p}$.

(i) *If $(-b/p) = 1$, then there exists a* PFLS *$u(a, b)$ reduced* modulo *p such that $(D/p) = 1$ and $\alpha(a, b, p) = d$ if and only if $d \mid (p-1)/2$, where $d \neq 1$.*

(ii) *If $(-b/p) = -1$, then there exists a* PFLS *$u(a, b)$ reduced* modulo *p such that $(D/p) = 1$ and $\alpha(a, b, p) = d$ if and only if $d \mid p - 1$ and $d \nmid (p-1)/2$.*

PROOF: (i) Firstly, $\alpha(a, b, p)$ can never equal 1, since $u_1 = 1$. Now, suppose that we have found a PFLS $u(a, b)$ such that $\alpha(a, b, p) = d$, where $d \neq 1$ is a positive integer dividing $p - 1$ and $(-b/p) = 1$. Then

$$r_2 = -b/r_1 \equiv gr_1 \pmod{p}$$

for some nonzero residue $g \not\equiv 1 \pmod{p}$. This leads to the congruence

$$r_1^2 \equiv -b/g \pmod{p}. \tag{8}$$

If $\alpha(a, b, p) = d$, then by Lemma 4(ii), d is the least positive integer such that $r_1^d \equiv r_2^d \pmod{p}$. Consequently, $\text{ord}_p(g) = d$. Since $(-b/p) = 1$, congruence (8) is solvable if and only if $(g/p) = 1$. But since $\text{ord}_p(g) = d$, $(g/p) = 1$ if and only if

$$d \mid (p - 1)/2.$$

By Lemma 6, we can now choose r_1 such that

$$r_1^2 \equiv -b/g \pmod{p},$$

where $\operatorname{ord}_p(g) = d$. Assertion (i) now follows.

(ii) This proof is similar to the proof of (i).

Before presenting Theorem 13, we will need Lemma 9, which is due to Wyler [8].

<u>*LEMMA 9 (Wyler):*</u> *Consider the* PFLS $u(a, b)$. *Suppose* $b \not\equiv 0 \pmod{p}$, *and let* $h = \operatorname{ord}_p(-b)$. *Suppose* $h = 2^c h'$, *where* h' *is an odd integer. Let*

$$k = \alpha(a, b, p) = 2^j k',$$

where k' *is an odd integer. Let* H *be the least common multiple of* h *and* k.

(i) $\mu(a, b, p) = H$ *or* $2H$; $\beta(a, b, p) = H/k$ *or* $2H/k$.

(ii) *If* $c \neq j$, *then* $\mu(a, b, p) = 2H$.
If $c = j > 0$, *then* $\mu(a, b, p) = H$.

<u>*THEOREM 13:*</u> *Let* p *be an odd prime of the form* $2^m q + 1$, *where* q *is an odd integer. Let* b *be a fixed integer such that* $b \not\equiv 0 \pmod{p}$. *Let* $h = \operatorname{ord}_p(-b) = 2^c h'$, *where* h' *is an odd integer.*

(i) *If* a *is an integer, then* $\beta(a, b, p) \mid 2h$ *for the* PFLS $u(a, b)$.

(ii) *If* $(-b/p) = -1$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid h'$.

(iii) *If* $(-b/p) = 1$, $h' \neq q$, *and either* $c = 0$ *or* $c < m - 1$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $B(a, b, p) = d$ *if and only if* $d \mid 2h$.

(iv) *If* $(-b/p) = 1$, $m \geqslant 2$, $c = m - 1$, *and* $h' \neq q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid 2h$ *and* $d \not\equiv 2 \pmod{4}$.

(v) *If* $(-b/p) = 1$, $m = 1$, *and* $h = q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid 2h$ *and* $h \nmid d$.

(vi) *If* $(-b/p) = 1$, $m \geqslant 2$, *and* $h = q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid 2h$ *and* $d \neq h$.

(vii) *If* $(-b/p) = 1$, $m = 2$, *and* $h = 2q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d \mid 2h$, $d \not\equiv 2 \pmod{4}$, *and* $h \nmid d$.

(viii) *If* $(-b/p) = 1$, $m \geqslant 3$, $1 \leqslant c < m - 1$, *and* $h' = q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d|2h$ *and* $d \neq 2h$.

(ix) *If* $(-b/p) = 1$, $m \geqslant 3$, $c = m - 1$, *and* $h' = q$, *then there exists a* PFLS $u(a, b)$ *reduced* modulo p *such that* $(D/p) = 1$ *and* $\beta(a, b, p) = d$ *if and only if* $d|2h$, $d \not\equiv 2 \pmod 4$, *and* $d \neq 2h$.

(x) *If there exists a* PFLS $u(a, b)$ *such that* $\beta(a, b, p) = d$ *and* s *is an integer such that* $\text{ord}_p(s) = d$, *then there exists a* PFLS $u(a, b)$ *such that* $s(a, b, p) \equiv s \pmod p$.

<u>*PROOF:*</u> (i) Let $k = \alpha(a, b, p)$. By the definition of $s(a, b, p)$ and (6),

$$s^2 = u_{k+1}^2 = u_{k+1}^2 - 0 \equiv u_{k+1}^2 - u_k u_{k+2} \equiv (-b)^k \pmod p.$$

Thus,

$$s^{2h} \equiv (-b)^{kh} \equiv ((-b)^h)^k \equiv 1 \equiv 1 \pmod p)$$

and $\text{ord}_p(s)$, which is equal to $\beta(a, b, p)$, divides $2h$.

(ii) Note that $(-b/p) = -1$ implies that $c = m$. Since $(-b/p) = -1$, it follows from Theorem 12(ii) that for any PFLS $u(a, b)$ such that $(D/p) = 1$, $\alpha(a, b, p) \nmid (p - 1)/2$, but $\alpha(a, b, p)|p - 1$. Thus,

$$2^m|\alpha(a, b, p).$$

By Theorem 11, $h = 2^c h'|\mu(a, b, p)$. Since $\alpha(a, b, p)|\mu(a, b, p)$, $\mu(a, b, p)|p - 1$, and $\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p)$, it follows that $\beta(a, b, p)$ is an odd integer. By part (i),

$$\beta(a, b, p)|2h.$$

Thus,

$$\beta(a, b, p)|h'.$$

Now suppose that $d|h'$. We wish to choose a residue r_1 such that

$$r_1^2 \equiv (-b)^{d+1} \pmod p. \tag{9}$$

One solution for r_1 is $(-b)^{(d+1)/2}$, since $d + 1$ is even. By Lemma 6, we can find a PFLS $u(a, b)$ whose characteristic root r_1 satisfies congruence (9). Now,

$$r_2 = -b/r_1 \equiv (-b)^{(1-d)/2} \pmod p.$$

Since $(d + 1)/2$ and $(1 - d)/2$ are relatively prime to each other and to h',

$$[\text{ord}_p(r_1), \text{ord}_p(r_2)] = \text{ord}_p(-b) = 2^c h'.$$

Thus, by Lemma 4(i), $\mu(a, b, p) = 2^c h'$. By Lemma 4(ii),

$$\alpha(a,\ b,\ p) = \text{ord}_p(r_1/r_2) = \text{ord}_p((-b)^{(d+1)/2}/(-b)^{(1-d)/2})$$
$$= \text{ord}_p((-b)^d) = 2^c h'/d.$$

Thus

$$\beta(a,\ b,\ p) = \mu(a,\ b,\ p)/\alpha(a,\ b,\ p) = d.$$

(iii) It follows from part (i) that if $\beta(a,\ b,\ p) = d$, then $d|2h$. If $d|2h$ and d is odd, then by the same argument as in the proof of part (ii), one can find a PFLS $u(a,\ b)$ such that $(D/p) = 1$,

$$\mu(a,\ b,\ p) = \text{ord}_p(-b),\ \alpha(a,\ b,\ p) = \text{ord}_p(-b)/d,$$

and

$$\beta(a,\ b,\ p) = d.$$

Now suppose that $c = 0$, $d|2h$, and $d \equiv 2 \pmod 4$. By what was stated above in this proof, we can find a PFLS $u(a,\ b)$ such that $(D/p) = 1$,

$$\mu(a,\ b,\ p) = h,\ \alpha(a,\ b,\ p) = h/(\tfrac{1}{2}d),$$

and

$$\beta(a,\ b,\ p) = d/2,$$

since $d/2$ is odd. Note that

$$\mu(a,\ b,\ p),\ \alpha(a,\ b,\ p),\text{ and }\beta(a,\ b,\ p)$$

are all odd. Since $\mu(a,\ b,\ p)$ is odd, $\text{ord}_p(s(a,\ b,\ p))$ is odd, and no power of $s(a,\ b,\ p)$ is congruent to -1 modulo p. Let $k = \alpha(a,\ b,\ p)$ and $s \equiv s(a,\ b,\ p) \pmod p$. Note that $u_{k+1} \equiv s \pmod p$ and $u_{gk+1} \equiv s^g \pmod p$, where g is a positive integer. One can easily verify that for the PFLS $u(a,\ b)$,

$$u_n(-a,\ b) = (-1)^{n-1}u_n(a,\ b).$$

It is clear that $\alpha(a,\ b,\ p) = \alpha(-a,\ b,\ p)$. Let $k' = \alpha(-a,\ b,\ p) = k$ and $s' = s(-a,\ b,\ p)$. Then $\mu(-a,\ b,\ p) = gk'$ for some positive integer g and

$$u_{gk'+1}(-a,\ b) \equiv (s')^g \equiv (-1)^{gk'}u_{gk'+1}(a,\ b)$$
$$\equiv (-1)^{gk}s^g \equiv 1 \pmod p.$$

Since $s^g \not\equiv -1 \pmod p$ and $\text{ord}_p(s) = d/2$, it follows that

$$g = \text{ord}_p(s') = d$$

and that $\beta(-a,\ b,\ p) = d$.

Now suppose that $c > 0$, $4|d$, and $d|2h$. Choose a residue n such that $n^2 \equiv -b \pmod{p}$. This is possible because $m > c$ and $h'|q$ imply that

$$(-b)^{(p-1)/2} \equiv (-b)^{2^{m-1}q} \equiv 1 \pmod{p}.$$

By Lemma 6, we can find a PFLS $u(a, b)$ whose characteristic root r_1 satisfies

$$r_1^2 \equiv n^{d+2} \pmod{p}.$$

One solution for r_1 is $n^{(d/2)+1}$, since d is even. Then

$$r_2 \equiv -b/r_1 \equiv n^{2-((d/2)+1)} \equiv n^{1-(d/2)} \pmod{p}.$$

Since $1 + (d/2) = -(1 - (d/2)) + 2$, the greatest common divisor of $1 + (d/2)$ and $1 - (d/2)$ must divide 2. Since $d/2$ is even, it follows that $1 + (d/2)$ and $1 - (d/2)$ are both odd, and thus relatively prime. Furthermore, $1 + (d/2)$ and $1 - (d/2)$ are both relatively prime to $\mathrm{ord}_p(n)$, which is equal to $2h$. Thus,

$$\mu(a, b, p) = [\mathrm{ord}_p(r_1), \mathrm{ord}_p(r_2)] = \mathrm{ord}_p(n) = 2h.$$

Further,

$$\alpha(a, b, p) = \mathrm{ord}_p(r_1/r_2) = \mathrm{ord}_p(n^{1+(d/2)}/n^{1-(d/2)})$$
$$= \mathrm{ord}_p(n^d) = 2h/d.$$

Thus,

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = d.$$

Finally, suppose that $c > 0$, $d|2h$, and $d \equiv 2 \pmod{4}$. Choose a residue f such that $f^4 \equiv -b \pmod{p}$. This is possible, since $c < m - 1$ and $h'|q$ imply that

$$(-b)^{(p-1)/4} \equiv (-b)^{2^{m-2}q} \equiv 1 \pmod{p}.$$

Note that $\mathrm{ord}_p(f)|4h$. By Lemma 6, we can find a PFLS $u(a, b)$ whose characteristic root r_1 satisfies

$$r_1^2 \equiv f^{d+4} \pmod{p}.$$

One solution for r_1 is $f^{(d/2)+2}$, since d is even. Then

$$r_1 = -b/r_1 \equiv f^{4-((d/2)+2)} \equiv f^{2-(d/2)} \pmod{p}.$$

Since $2 + (d/2) = -(2 - (d/2)) + 4$, the greatest common divisor of $2 + (d/2)$ and $2 - (d/2)$ must divide 4. Since $d \equiv 2 \pmod{4}$, $d/2$ is odd. Consequently, $2 - (d/2)$ and $2 + (d/2)$ are both odd and therefore both are relatively prime to $4h$, since $d|2h$. Thus,

$$\mu(a, b, p) = [\mathrm{ord}_p(r_1), \mathrm{ord}_p(r_2)] = \mathrm{ord}_p(f).$$

Further,

$$\alpha(a, b, p) = \mathrm{ord}_p(r_1/r_2) = \mathrm{ord}_p(f^{2+(d/2)}/f^{2-(d/2)})$$
$$= \mathrm{ord}_p(f^d) = 4 \cdot \mathrm{ord}_p(f)/d.$$

Hence,

$$\beta(a, b, p) = \mu(a, b, p)/\alpha(a, b, p) = d.$$

(iv) Suppose that there exists a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = d$, where $d|2h$ and $d \equiv 2 \pmod 4$. Further, suppose $2^{m-1}\|\alpha(a, b, p)$, where $2^k\|n$ means that $2^k|n$ but $2^{k+1}\nmid n$. Then, by Lemma 9, $\mu(a, b, p) = H$, where

$$H = [\mathrm{ord}_p(-b), \alpha(a, b, p)].$$

Thus,

$$2^{m-1}\|\mu(a, b, p) \quad \text{and} \quad 2^0\|\beta(a, b, p),$$

which is a contradiction. Now suppose that $2^e\|\alpha(a, b, p)$ where $e \leqslant m - 2$. Then by Lemma 9, $\mu(a, b, p) = 2H$ and $4|\beta(a, b, p)$, which again is a contradiction. Now suppose that $2^m\|\alpha(a, b, p)$. Then by Lemma 9, $\mu(a, b, p) = 2H$ and $2^{m+1}\|\mu(a, b, p)$. This contradicts the fact that $(D/p) = 1$, which implies $\mu(a, b, p)|p - 1$. Therefore, $\beta(a, b, p) \not\equiv 2 \pmod 4$ for any PFLS $u(a, b)$ such that $(D/p) = 1$. The rest of this proof is similar to the proofs of parts (ii) and (iii).

(v) Suppose that there exists a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = q$ or $\beta(a, b, p) = 2q$. If $f|\alpha(a, b, p)$, where $f|q$ and $f > 1$, then by Lemma 9, $\mu(a, b, p) = H$ or $2H$, and q/f is the largest odd divisor of $\beta(a, b, p)$. This contradicts the fact that $q|\beta(a, b, p)$. Further, $\alpha(a, b, p) \neq 1$. Thus, $\alpha(a, b, p) = 2$. In this case, $\mu(a, b, p) = 2H$ by Lemma 9, and $4|\mu(a, b, p)$. However, this contradicts the fact that $(D/p) = 1$, which implies $\mu(a, b, p)|p - 1$. Thus, $q\nmid\beta(a, b, p)$. The rest of the proof is similar to the proofs of parts (ii) and (iii).

(vi) We shall exhibit a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = 2q$. By Theorem 12(i), we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2$, since $m \geqslant 2$ and thus $2|(p - 1)/2$. By Lemma 9, $\mu(a, b, p) = 2H = 4q$, which divides $p - 1$. Hence, $\beta(a, b, p) = 2q$. The rest of the proof is similar to proofs of parts (ii), (iii), and (iv).

(vii) We shall exhibit a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = q$. By Theorem 12(i), we can find a PFLS $u(a, b)$ such that $(D/p\ ) = 1$ and $\alpha(a, b, p) = 2$. By Lemma 9, $\mu(a, b, p) = H = 2q$

$\beta(a, b, p) = q$. The rest of the proof is similar to proofs of parts (ii)-(v).

(viii) We shall exhibit a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\beta(a, b, p) = 2^e q$, where $0 \leqslant e \leqslant c$. If $1 < e \leqslant c$, then by Theorem 12(i) we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2^{c-e+1}$, since $2^{c-e+1} | (p - 1)/2$. By Lemma 9, $\mu(a, b, p) = 2H = 2^{c+1}q$ and $\beta(a, b, p) = 2^e q$. If $e = 1$, then by Theorem 12(i) we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2^{c+1}$, since $2^{c+1} | (p-1)/2$. By Lemma 9, $\mu(a, b, p) = 2H = 2^{c+2}q$ and $\mu(a, b, p) | p - 1$, which is consistent with $(D/p) = 1$. It follows that $\beta(a, b, p) = 2q$. If $e = 0$, then by Theorem 12(i) we can find a PFLS $u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = 2^c$. By Lemma 9, $\mu(a, b, p) = H = 2^c q$ and $\beta(a, b, p) = q$. The rest of the proof is similar to proofs of parts (ii), (iii), and (v).

(ix) This proof is similar to proofs of parts (ii)-(v) and (viii).

(x) This proof is similar to that of Theorem 6.

9. THE CASE FOR WHICH a IS A FIXED INTEGER

I am unable to obtain such definitive results given the parameter a as were obtained given the parameter b. The reason is that $r_1 r_2 = -b$, while $r_1 + r_2 = a$, and it is frequently easier to obtain multiplicative results in number theory than additive results. We now present two theorems, Theorems 14 and 15. Theorem 14 is complete, while Theorem 15 is not as comprehensive as the corresponding result in the preceding section.

THEOREM 14: *Let p be an odd prime and let a be any fixed integer. If $a \equiv 0 \pmod{p}$, then for any integer b such that $b \not\equiv 0 \pmod{p}$, $\alpha(a, b, p) = 2$. If $a \not\equiv 0 \pmod{p}$, $d | p - 1$, and $d \nmid 2$, then there exists a* PFLS *$u(a, b)$ such that $(D/p) = 1$ and $\alpha(a, b, p) = d$.*

PROOF: If $a \equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$, it is obvious that $\alpha(a, b, p) = 2$. Suppose that $a \not\equiv 0 \pmod{p}$, $d | p - 1$, and $d \nmid 2$. Let s be an integer such that $\operatorname{ord}_p(s) = d$. We wish to find residues r_1 and r_2 that satisfy the simultaneous congruences

$$\begin{aligned} r_1 + r_2 &\equiv a \pmod{p} \\ r_1/r_2 &\equiv s \pmod{p} \end{aligned} \tag{10}$$

which lead to the simultaneous congruences

$$\begin{aligned} r_1 + r_2 &\equiv a \pmod{p} \\ r_1 - r_2 s &\equiv 0 \pmod{p}. \end{aligned} \tag{11}$$

By Cramer's rule, if $a \not\equiv 0 \pmod{p}$, then (11) is solvable if and only if

$$-r_1r_2s - r_1r_2 \not\equiv 0 \pmod{p}.$$

Now, $-r_1r_2s - r_1r_2 \equiv 0 \pmod{p}$ if and only if $s \equiv -1 \pmod{p}$, which implies that $d = 2$. However, this case is ruled out by hypothesis. Thus, (10) is solvable. Now, by Lemma 7, we can find a PFLS $u(a, b)$ such that $r_1 + r_2 \equiv a \pmod{p}$ and $r_1/r_2 \equiv s \pmod{p}$. Then

$$\alpha(a, b, p) = \text{ord}_p(r_1/r_2) = \text{ord}_p(s) = d$$

and we are done.

<u>*THEOREM 15:*</u> *Let p be an odd prime and a be any integer. Look at the collection*

$$a - 1,\ a - 2,\ a - 3,\ \ldots,\ a - (p - 1).$$

Then there exists a PFLS *$u(a, b)$ such that $b \not\equiv 0 \pmod{p}$, $(D/p) = 1$, and $\mu(a, b, p) = m$, where m is any of the numbers*

$$[\text{ord}_p(a - r_i),\ \text{ord}_p(r_i)],\ 1 \leqslant r_i \leqslant p - 1,\ r_i \not\equiv a/2 \pmod{p}.$$

In particular, if $p > 3$, then, given any integer a, there exist at least $(\phi(p - 1))/2$ PFLS's *$u(a, b)$ reduced* modulo *p such that $b \not\equiv 0 \pmod{p}$, $(D/p) = 1$, and $u(a, b)$ has a maximal period* modulo *p of $p - 1$.*

<u>*PROOF:*</u> This follows from the fact that $r_1 + r_2 = a$ and from Lemmas 4(i) and 7. Note that by hypothesis, $r_1 \not\equiv r_2 \pmod{p}$, which is satisfied if and only if $r_1 \not\equiv a/2 \pmod{p}$. The last assertion follows from the fact that there are $\phi(p - 1)$ residues modulo p belonging to the exponent $p - 1$. Excluding the residue $a/2$ modulo p leaves at least $\phi(p - 1) - 1$ residues remaining with a maximal exponent of $p - 1$. Since $p > 3$, $\phi(p - 1) - 1$ is a positive odd integer. Since a PFLS $u(a, b)$ might have both its characteristic roots r_1 and r_2 with exponents of $p - 1$, these residues correspond to at least

$$(\phi(p - 1) - 2)/2 + 1$$

distinct PFLS's $u(a, b)$ modulo p. The result now follows.

The reason I was not able to obtain a more definitive result for Theorem 15 was that for a PFLS $u(a, b)$, $\mu(a, b, p)$ is determined by

$$[\text{ord}_p(r_1),\ \text{ord}_p(r_2)],\ \text{where } r_1 + r_2 = a.$$

However, I was not able to find any clear relationship between the exponents of r_1 and $a - r_1$ modulo p, which limited the scope of the theorem.

ACKNOWLEDGMENT

I wish to express my appreciation to Professor Harald Niederreiter for suggestions leading to the improvement of Theorem 14.

REFERENCES

1. Robert P. Backstrom. "On the Determination of the Zeros of the Fibonacci Sequence." *The Fibonacci Quarterly* 4, No. 4 (Dec. 1966):313-322.
2. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n + \beta^n$." *Ann. Math.* Second Series, 15 (1913):30-70.
3. Marshall Hall. "Divisors of Second-Order Sequences." *Bull. Amer. Math. Soc.* 43 (1937):78-80.
4. John H. Halton. "On the Divisibility Properties of Fibonacci Numbers." *The Fibonacci Quarterly* 4, No. 3 (Oct. 1966):217-240.
5. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. Math.* Second Series, 31 (1930):419-488.
6. Lawrence Somer. "Fibonacci-Like Groups and Periods of Fibonacci-Like Sequences." *The Fibonacci Quarterly* 15, No. 1 (Feb. 1977):35-41.
7. Morgan Ward. "Note on the Period of a Mark in a Finite Field." *Bull. Amer. Math. Soc.* 40 (1934):279-281.
8. Oswald Wyler. "On Second-Order Recurrences." *Amer. Math. Monthly* 72 (1965):500-506.

*****