THE DIVISIBILITY PROPERTIES OF PRIMARY LUCAS RECURRENCES WITH RESPECT TO PRIMES

LAWRENCE SOMER
U.S. Dept. of Agriculture, FSQS, Washington, D.C. 20250

1. INTRODUCTION

In this paper we will extend the results of D. D. Wall [12], John Vinson [11], D. W. Robinson [9], and John H. Halton [3] concerning the divisibility properties of the Fibonacci sequence to the general Lucas sequence

$$(r_1^n - r_2^n)/(r_1 - r_2).$$

In particular, we will improve their theorems for the Fibonacci sequence. Their results are inconclusive for those primes for which

$$(5/p) = (-1/p) = 1,$$

where (x/p) is the Legendre symbol for the quadratic character of x with respect to the prime p. We will obtain sharper results in these cases.

Let

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

where u_0, u_1, a, and b are integers, be an integral second-order linear recurrence. The integers a and b will be called the parameters of the recurrence. If $u_0 = 0$ and $u_1 = 1$, such a recurrence will be called a primary recurrence (PR) and will be denoted by $u(a, b)$. Associated with PR $u(a, b)$ is its characteristic polynomial

$$x^2 - ax - b = 0$$

with roots r_1 and r_2 where $r_1 + r_2 = a$ and $r_1 r_2 = -b$. Let

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

be the discriminant of the characteristic polynomial. If $D \neq 0$, then, by the Binet formula

$$u_n = (r_1^n - r_2^n)/(r_1 - r_2). \tag{2}$$

One other type of sequence will be of interest: the Lucas sequence $v(a, b)$ in which

$$v_{n+2} = av_{n+1} + bv_n,\ v_0 = 2,\ v_1 = a. \tag{3}$$

As is well known, the Lucas sequence is given by the Binet formula

$$v_n = r_1^n + r_2^n. \tag{4}$$

To continue, we need the following definitions which are modeled after the notation of Halton [3]. The letter p will always denote a rational prime.

Definition 1: $\nu(a, b, p)$ is the numeric of the PR $u(a, b)$ modulo p. It is the number of nonrepeating terms modulo p.

Definition 2: $\mu(a, b, p)$ is the period of the PR $u(a, b)$ modulo p. It is the least positive integer k such that

$$u_{n+k} \equiv u_n \pmod p$$

is true for all $n \geq \nu(a, b, p)$.

Clearly, if $\nu(a, b, p) = 0$,

$$u_{\mu(a,b,p)} \equiv 0 \quad \text{and} \quad u_{\mu(a,b,p)+1} \equiv 1 \pmod p.$$

Definition 3: $\alpha(a, b, p)$ is the restricted period of the PR $u(a, b)$ modulo p. It is the least positive integer k such that

$$u_{n+k} \equiv su_n \pmod{p}$$

for all $n \geq \nu(a, b, p)$ and some nonzero residue s. Then $s = s(a, b, p)$ is called the multiplier of the PR $u(a,b)$. If $u_k \equiv 0 \pmod{p}$ for $k \geq \nu(a, b, p)$, we say that $s(a, b, p) = 0$ by convention.

Definition 4: $\beta(a, b, p)$ is called the exponent of the multiplier $s(a, b, p)$ modulo p. It is clearly equal to

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

Definition 5: In the PR $u(a, b)$ the rank of apparition of p is the least positive integer, if it exists, such that $u_k \equiv 0 \pmod{p}$.

We will restrict our attention chiefly to the PR's $u(a, b)$, because, as we shall see, if $b \neq 0$, then for these sequences the rank of apparition of p exists. By [10], primary recurrences are essentially the only recurrences having this property.

2. PRELIMINARY RESULTS

The following well-known properties of Lucas sequences will be necessary for our future proofs. Proofs of these results can be found in the papers of Lucas [8] or Carmichael [2].

(5) In the PR $u(a, b)$ suppose that $b \not\equiv 0 \pmod{p}$ and that $p \neq 2$. Then

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

(6) $$u_{m+n} = bu_m u_{n-1} + u_n u_{m+1}.$$

(7) $$u_n^2 - u_{n-1}u_{n+1} = (-b)^{n-1},\ n \geq 1.$$

(8) $$v_n^2 - Du_n^2 = 4(-b)^n.$$

(9) $$u_{2n} = u_n v_n.$$

(10) If $p \nmid bD$, then p is a divisor of the Lucas sequence $v(a, b)$ if and only if $\alpha(a, b, p) \equiv 0 \pmod{2}$ for the PR $u(a, b)$. Then the rank of apparition of p in $v(a, b)$ is $(1/2)\alpha(a, b, p)$.

The following two lemmas will determine the possible numerics $\nu(a, b, p)$ for the PR $u(a, b)$ modulo p.

Lemma 1: In the PR $u(a, b)$ if $b \not\equiv 0 \pmod{p}$, then $\nu(a, b, p) = 0$ and $\alpha(a, b, p)$ is also the rank of apparition of p. Also, if $u_k \equiv 0 \pmod{p}$, then

$$\alpha(a, b, p) | k.$$

Further

$$\alpha(a, b, p) | p - (D/p).$$

Proof: Since there are only p^2 possible pairs of consecutive terms $(u_n, u_{n+1}) \pmod{p}$, some pair must repeat. Suppose that the pair (u_k, u_{k+1}) is the first such pair to repeat modulo p and that $k \neq 0$. Let $m = \mu(a, b, p)$. Then,

$$u_{k+m} \equiv u_k \quad\text{and}\quad u_{k+1+m} \equiv u_{k+1} \pmod{p}.$$

However, by the recurrence relation (1),

$$bu_{k-1} \equiv u_{k+1} - au_k.$$

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

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

Hence, the pair (u_{k-1}, u_k) repeats modulo p which is a contradiction if $k \neq 0$. Thus, the pair $(u_0, u_1) = (0, 1)$ repeats modulo p. Hence, the numeric is 0 modulo p and the PR $u(a, b)$ is purely periodic modulo p.

Now, let $n = \alpha(a, b, p)$. As in the above argument, (u_0, u_1) is the first pair (u_k, u_{k+1}) such that

$$u_{k+n} \equiv su_k \quad \text{and} \quad u_{k+1+n} \equiv su_{k+1} \pmod p$$

for some residue $s \pmod p$. The assertion that $\alpha(a, b, p) | k$ now follows from the fact that the PR $u(a, b)$ is purely periodic modulo p. The rest of the lemma follows from (5).

Lemma 2: In the PR $u(a, b)$, assume that $b \equiv 0 \pmod p$.

(i) If $a \not\equiv 0 \pmod p$, then $\nu(a, b, p) = 1$ and $u_n \equiv a^{n-1} \pmod p$, $n \geq 1$.

(ii) If $a \equiv 0 \pmod p$, then $\nu(a, b, p) = 2$ and $u_n \equiv 0 \pmod p$, $n \geq 2$.

Proof: This follows by simple verification.

3. RESULTS FOR SPECIAL CASES

For certain special classes of PR's, we can easily determine $\mu(a, b, p)$, $\alpha(a, b, p)$, and $s(a, b, p)$. Of course, if $\mu(a, b, p)$ and $\alpha(a, b, p)$ are known exactly, $\beta(a, b, p)$ is immediately determined. Theorems 1-4 will discuss these cases. The proofs follow by induction and direct verification.

Theorem 1: In the PR $u(a, b)$, suppose that $b = 0$.

(i) If $a \not\equiv 0 \pmod p$, then $u_n = a^{n-1}$, $n \geq 1$.

Further,

$$\nu(a, b, p) = 1,\ \alpha(a, b, p) = 1,\ \mu(a, b, p) = \operatorname{ord}_p(a), \text{ and } s(a, b, p) = a$$

for all primes p, where $\operatorname{ord}_p(x)$ denotes the exponent of x modulo p.

(ii) If $a \equiv 0 \pmod p$, then $u_n = 0$, $n \geq 2$,

$$\nu(a, b, p) = 2,\ \alpha(a, b, p) = 1,\ \mu(a, b, p) = 1, \text{ and } s(a, b, p) = 0.$$

Theorem 2: In the PR $u(a, b)$ let $a = 0$ and $b \not\equiv 0 \pmod p$. Then

$$u_{2n} = 0 \quad \text{and} \quad u_{2n+1} = b,\ n \geq 0.$$

Further,

$$\nu(a, b, p) = 0,\ \alpha(a, b, p) = 2,\ \mu(a, b, p) = 2 \operatorname{ord}_p(b), \text{ and } s(a, b, p) = b.$$

Theorem 3: In the PR $u(a, b)$ suppose that $D = 0$, $a \not\equiv 0 \pmod p$, and $b \not\equiv 0 \pmod p$. Then

$$u_n = n(a/2)^{n-1},\ n \geq 0.$$

Further

$$\alpha(a, b, p) = p,\ \mu(a, b, p) = p \operatorname{ord}_p(a/2), \text{ and } s(a, b, p) = a/2.$$

Theorem 4: In the PR $u(a, b)$ suppose that r_1/r_2 is a root of unity. Let k be the order of the root of unity. Let ζ_k be a primitive kth root of unity.

(i) If $k = 1$, then $a = 2N$, $b = -N$, $D = 0$, $r_1 = N$, $r_2 = N$, and $r_1/r_2 = 1$. Theorem 3 characterizes the terms of this sequence.

(ii) If $k = 2$, then $a = 0$, $b = N$, $D = 4N$, $r_1 = \sqrt{N}$, $r_2 = -\sqrt{N}$, and $r_1/r_2 = -1$. Theorem 2 characterizes the terms of this sequence.

(iii) If $k = 3$, $a = N$, $b = -N^2$, $D = -3N^2$, $r_1 = -\zeta_3 N$, $r_2 = -\zeta_3^2 N$, and $r_1/r_2 = \zeta_3^{-1}$.

(iv) If $k = 4$, $a = 2N$, $b = -2N^2$, $D = -4N^2$, $r_1 = (1 + i)N$, $r_2 = (1 - i)N$, and $r_1/r_2 = i$ where $i = \sqrt{-1}$.

(v) If $k = 6$, $a = 3N$, $b = -3N^2$, $D = -3N^2$, $r_1 = -i\zeta_3\sqrt{3}$, $r_2 = i\zeta_3^2(\sqrt{3})N$, and $r_1/r_2 = \zeta_6$.

Moreover, if $k \geq 2$, then

$$\alpha(a, b, p) = k, \ \mu(a, b, p) = k \ \mathrm{ord}_p(s),$$

and

$$s(a, b, p) = s \equiv \mathrm{sgn}(a^k)(-(-b)^{k/2}) \pmod p,$$

where $\mathrm{sgn}(x)$ denotes the sign of x. Furthermore, if $n = qk + r$, $0 \geq r \geq k$, and $k \geq 3$, then

$$u_n = s^q u_r = (-1)^q N^{qk} u_r.$$

In Theorem 4, note that $k = 1, 2, 3, 4$, or 6 are the only possibilities for k since these are the only orders of roots of unity that satisfy a quadratic polynomial over the rationals.

Just as we treated the divisibility properties of certain special recurrences with respect to a general prime, we now consider the special case of the prime 2 in the following theorem. We have already handled the cases where $b \equiv 0$ or $a \equiv 0 \pmod 2$ in Theorems 1 and 2.

Theorem 5: Consider the PR $u(a, b)$. Suppose that $2 \nmid ab$. Then $\nu(a, b, 2) = 0$, $\mu(a, b, 2) = 3$, $\alpha(a, b, 2) = 3$, and $s(a, b, 2) = 1$. The reduced recurrence modulo 2 is then

$$(0, 1, 1, 0, 1, 1, \ldots) \pmod 2.$$

4. GENERAL RESULTS

From this point on, p will always denote an odd prime unless otherwise specified. Theorem 6 gives criteria for determining $\mu(a, b, p)$, $\alpha(a, b, p)$, and $s(a, b, p)$ for the general PR $u(a, b)$. For the rest of the paper, D' will denote the square-free part of the discriminant D, and K will denote the algebraic number field $Q(\sqrt{D'})$, where Q as usual stands for the rationals.

Theorem 6: In the PR $u(a, b)$, suppose that $p \mid bD$. Let P be a prime ideal in K dividing p. If $(D/p) = 1$, we will identify P with p.

(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. If $(D/p) = -1$, then $\alpha(a, b, p)$ is also the least positive integer n such that r_1 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 is well-defined modulo P. Further, 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 also well-defined modulo P.

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

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

and

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

Thus, $r_1^n \equiv r_2^n \pmod P$. Hence,

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

Thus, $r_1^n \equiv r_2^n \equiv 1 \pmod P$. Conversely, if $r_1^k \equiv r_2^k \equiv 1 \pmod P$ for some positive integer k, then it follows that $u_k \equiv 0$ 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

$$(r_1/r_2)^n \equiv 1 \pmod P.$$

Hence, $\alpha(a, b, p)$ is the exponent of r_1/r_2 modulo P.

Further, if $(D/p) = -1$, then

$$\sigma(r_1) = r_1^p \equiv r_2 \pmod{P} \quad\text{and}\quad \sigma(r_1^n) = (r_1^p)^n \equiv r_2^n \pmod{P},$$

where σ is the Frobenius automorphism of R/P. This follows, since r_1 and r_2 are both roots of the irreducible polynomial modulo P, $x^2 - ax - b$. Thus, if $r_1^n \equiv r_2^n \pmod{P}$, we obtain

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

Let Z_p denote the finite field of p elements. Now,

$$R/P = Z_p[\sqrt{D'}].$$

In $Z_p[\sqrt{D'}]$, the only solutions of the equation $x^p - x = 0$ are those in Z_p by Fermat's theorem. 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,

$$\begin{aligned} u_{k+1} = (r_1^{k+1} - r_2^{k+1})/(r_1 - r_2) &\equiv (r_1^k(r_1) - r_1^k(r_2))/(r_1 - r_2) \\ &\equiv r_1^k \equiv s(a, b, p) \pmod{P}. \end{aligned}$$

The proof is now complete.

Theorem 6, while definitive, is impractical for actually computing

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

We will develop more practical methods of determining these numbers, although our results will not be as complete. The most easily applied of our methods will use the quadratic character modulo p and pertain to certain special classes of PR's. For sharper results, we will also utilize the less convenient 2^n-*ic* characters modulo p.

A good theory of the divisibility properties of the PR $u(a, b)$ with respect to p should give limitations for the restricted period modulo p. Given the restricted period, one should then be able to determine exactly the exponent of the multiplier modulo p and, consequently, the period modulo p. Further, we should be able to specify the multiplier modulo p. This will be our program from here on. As a first step toward fulfilling this project, we now present Theorems 7 and 8. Theorem 7 is due to Wyler [14] and, in most cases, determines $\mu(a, b, p)$ when $\alpha(a, b, p)$ and $\mathrm{ord}_p(-b)$ are known. Theorem 8 is the author's application of Wyler's Theorem 7.

Theorem 7: Consider the PR $u(a, b)$. Suppose $b \not\equiv 0 \pmod{p}$. Let $h = \mathrm{ord}_p(-b)$. Suppose $h = 2^c h'$, where h' is an odd integer. Let $k = \alpha(a, b, p) = 2^d k'$, 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 $c \neq d$, then $\mu(a, b, p) = 2H$. If $c = d > 0$, then $\mu(a, b, p) = H$.

This theorem is complete in the sense that if $c = d = 0$, then $\mu(a, b, p)$ may be either H or $2H$. For example, look at the PR $u(3, -1)$. For all primes p, $h = \mathrm{ord}_p(1) = 1 = 2^0(1)$.

If $p = 13$, then $k = \alpha(3, -1, 13) = 7 = 2^0(7)$. Further, $H = [1, 7] = 7$. By inspection, $\mu(3, -1, 13) = 14 = 2H$.

If $p = 29$, then $k = \alpha(3, -1, 29) = 7$. As before, $H = 7$. But now we have $\mu(3, -1, 29) = 7 = H$.

Theorem 8: Let p be an odd prime. Consider the PR $u(a, b)$, where $b \not\equiv 0 \pmod{p}$. Let $h = \mathrm{ord}_p(-b)$. Suppose $h = 2^c h'$, where h' is an odd integer. Let $k = \alpha(a, b, p) = 2^d k'$, where k' is an odd integer. Let $H = [h, k]$, where $[x, y]$ is the least common multiple of x and y. Let $s = s(a, b, p)$.

(i) $s^2 \equiv (-b)^k \pmod{p}$.
(ii) If $c = d = 0$ and $\mu(a, b, p) = H$, then $s \equiv (-b)^{(k+h)/2} \pmod{p}$.
(iii) If $c = d = 0$ and $\mu(a, b, p) = 2H$, then $s \equiv -(-b)^{(k+h)/2} \pmod{p}$.
(iv) If $c = d > 0$, then $s \equiv -(-b)^{k/2} \pmod{p}$.
(v) If $d > c$, then $s \equiv -(-b)^{k/2} \pmod{p}$.
(vi) If $c > d$, then $s \equiv \pm r$, where $r^2 \equiv (-b)^k \pmod{p}$ and $0 \leq r \leq (p-1)/2$.
Further, both possibilities do in fact occur.

Proof:
(i) This follows immediately from (7), letting $n = k$.
(ii) Let $c = d = 0$ and assume that $\mu(a, b, p) = H$. Then,

$$\text{ord}_p(s) = \beta(a, b, p) = H/k = [h, k]/k.$$

Further, by (i),

$$s^2 \equiv (-b)^k \pmod{p}.$$

Thus,

$$s \equiv (-b)^{(k+h)/2} \quad \text{or} \quad s \equiv -(-b)^{(k+h)/2} \pmod{p}.$$

In general, it is easy to see that if r is a positive integer,

$$\text{ord}_p(-b)^r = [h, r]/r.$$

Therefore,

$$\text{ord}_p((-b)^{(k+h)/2}) = [h, (k+h)/2]/((k+h)/2).$$

Suppose $g = (h, k)$. Let $h = gm$ and $k = gn$, where $(m, n) = 1$. Then,

$$\begin{aligned}[h, (k+h)/2]/((k+h)/2) &= [gm, g(m+n)/2]/(g(m+n)/2)\\ &= g[m, (m+n)/2]/(g(m+n)/2).\end{aligned}$$

Clearly, $(m, m+n) = 1$ and, a fortiori, $(m, (m+n)/2) = 1$. Hence,

$$g[m, (m+n)/2]/(g(m+n)/2) = (gm(m+n)/2)/(g(m+n)/2) = m.$$

But,

$$[h, k]/k = [gm, gn]/(gn) = gmn/(gn) = m.$$

Thus,

$$\text{ord}_p((-b)^{(k+h)/2}) = \text{ord}_p(s) = m.$$

However, since m is odd,

$$\text{ord}_p(-(-b)^{(k+h)/2}) = 2m.$$

Thus, $s \equiv (-b)^{(k+h)/2} \pmod{p}$.

(iii)-(v) The proofs of these assertions are similar to that of (ii). In calculating $\text{ord}_p(s)$ for (iv) and (v), we make use of Wyler's Theorem 7.

(vi) To see that both possibilities actually occur, consider $s(1, 1, 13)$ and $s(1, 1, 17)$.

Now, $\alpha(1, 1, 13) = 7$ and $\text{ord}_{13}(-1) = 2$, so $c > d$. By inspection, we see that

$$s(1, 1, 13) \equiv 8 > (13-1)/2 = 6 \pmod{13}.$$

Also, $\alpha(1, 1, 17) = 9$ and $\text{ord}_{17}(-1) = 2$. Hence, $c > d$. However, we now find that

$$s(1, 1, 17) \equiv 4 \leq (17-1)/2 = 8 \pmod{17},$$

and we are done.

Unfortunately, Theorems 7 and 8 depend on knowing the highest power of 2 dividing $\alpha(a, b, p)$ and $\text{ord}_p(-b)$ to determine $\beta(a, b, p)$ and $\mu(a, b, p)$. Our project will be to find classes of PR's (excluding the special cases already treated) in which for almost all primes p the exponent of the multiplier modulo p, $\beta(a, b, p)$, can be determined by knowing the residue class modulo m to which $\alpha(a, b, p)$ belongs for some fixed positive integer m. In addition, we would like a set of conditions, preferably involving the quadratic character modulo p, for determining $\alpha(a, b, p)$ modulo m without explicitly computing $\alpha(a, b, p)$.

By Theorem 7, these conditions can be satisfied if either

(i) $\text{ord}_p(-b)\,|\,m$ for a fixed positive integer m and for almost all primes p, or

(ii) $2H/\alpha(a, b, p)\,|\,m$ for a fixed positive integer m and for almost all primes p.

Now, condition (i) can be satisfied for almost all p iff $b = \pm 1$. Thus, we will consider the PR's $u(a, 1)$ and $u(a, -1)$. If $b = 1$, then $\text{ord}_p(-b) = 2$ for all odd primes p and, by Theorem 7, $H = \alpha(a, 1, p)$ or $H = 2\alpha(a, 1, p)$. Hence, $\beta(a, 1, p)\,|\,4$ and $\beta(a, 1, p)$ is largely determined if $\alpha(a, 1, p)$ is known modulo 4. Similarly, if $b = -1$, then $\beta(a, -1, p)$ is largely determined if $\alpha(a, -1, p)$ is known modulo 2.

By Theorems 6 and 7, $H = [\text{ord}_p(r_1/r_2), \text{ord}_p(-b)]$. Hence, condition (ii) can be satisfied if

$$r_1/r_2 = \pm b. \tag{11}$$

Since $r_1 r_2 = -b$, equation (11) is equivalent to requiring that

$$r_1/r_2 = \pm r_1 r_2. \tag{12}$$

Solving, we see that $r_2^2 = 1$ or $r_2^2 = -1$. But, if $r_2^2 = -1$, then $r_2 = \pm i$ and $r_1 = \mp i$. However, this case is already treated by Theorem 4(ii). If $r_2^2 = 1$, then $r_2 = \pm 1$. If $r_2 = 1$, then by Theorem 6 we see that $\beta(a, b, p) = 1$ always no matter what $\alpha(a, b, p)$ is. If $r_2 = -1$, then Theorem 6 and a little analysis shows that $\beta(a, b, p)\,|\,2$ and depends upon the residue class of $\alpha(a, b, p)$ modulo 2. Note that if $r_2 = 1$, then

$$r_1 = -b/r_2 = -b \quad \text{and} \quad a = r_1 + r_2 = -b + 1. \tag{13}$$

If $r_2 = -1$, then

$$r_1 = b \quad \text{and} \quad a = b - 1. \tag{14}$$

Hence, we will also investigate the divisibility properties of the PR's

$$u(-b + 1, b) \quad \text{and} \quad u(b - 1, b).$$

From our preceding discussion, it will be very helpful if we can find conditions to determine $\alpha(a, b, p)$ modulo 4. The following two lemmas and two theorems determine the residue class of $\alpha(a, b, p)$ modulo 4 for a general PR $u(a, b)$.

Lemma 3: Let p be an odd prime. Consider the PR $u(a, b)$. Suppose that $p \nmid bD$.

(i) If $\alpha(a, b, p) \equiv 1 \pmod 2$, then $(-b/p) = 1$.

(ii) If $\alpha(a, b, p) \equiv 2 \pmod 4$, then $(bD/p) = 1$.

(iii) If $\alpha(a, b, p) \equiv 0 \pmod 4$, then $(bD/p) = (-b/p)$.

Proof: Firstly, note that by (8),

$$v_n^2 - Du_n^2 = 4(-b)^n. \tag{15}$$

(i) Let $k = \alpha(a, b, p) \equiv 1 \pmod 2$. By (15),

$$v_k^2 \equiv 4(-b)^k \pmod p.$$

Since $k \equiv 1 \pmod 2$, this is possible only if $(-b/p) = 1$.

(ii) Let $2k = \alpha(a, b, p)$. Then $k \equiv 1 \pmod 2$. By (10), $v_k \equiv 0 \pmod p$. Then by (15),

$$-Du_k^2 \equiv 4(-b)^k \pmod p.$$

If $(-b/p) = 1$, then clearly, $(-D/p) = 1$. If $(-b/p) = -1$, then $(-D/p) = -1$, since $k \equiv 1 \pmod 2$. In both cases, $(bD/p) = 1$.

(iii) Let $2k = \alpha(a, b, p)$. Then $k \equiv 0 \pmod 2$. By (10), $v_k \equiv 0 \pmod p$. Then by (15),

$$-Du_k^2 \equiv 4(-b)^k \pmod p.$$

Since $k \equiv 0 \pmod 2$, $(-D/p) = 1$ in all cases. It follows that $(bD/p) = (-b/p)$.

Theorem 9: Let p be an odd prime. Consider the PR $u(a, b)$. Suppose $p \nmid bD$.

(i) If $(-b/p) = 1$ and $(bD/p) = -1$, then $\alpha(a, b, p) \equiv 1 \pmod 2$.

(ii) If $(-b/p) = -1$ and $(bD/p) = 1$, then $\alpha(a, b, p) \equiv 2 \pmod 4$.

(iii) If $(-b/p) = (bD/p) = -1$, then $\alpha(a, b, p) \equiv 0 \pmod 4$.

Proof: This follows immediately from Lemma 3.

As we can see from Theorem 9, the only doubtful case occurs when

$$(-b/p) = (bD/p) = 1.$$

Lemma 4 and Theorem 10 give a new criterion for determining the restricted period in some instances when $(-b/p) = (bD/p) = 1$.

Lemma 4: Let p be an odd prime. Consider the PR $u(a, b)$. Suppose $p \nmid bD$ and $\alpha(a, b, p) \equiv 1 \pmod 2$. Then $(-b/p) = 1$. Let $r^2 \equiv -b$, where $0 \le r \le (p-1)/2$. Then

$$(-2b + ar/p) = 1 \quad \text{or} \quad (-2b - ar/p) = 1, \tag{16}$$

where $(-2b + ar/p)$ denotes the Legendre symbol.

Proof: By Lemma 3(i), we know that $(-b/p) = 1$. Let $k = \alpha(a, b, p)$. By (6),

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

Hence,

$$u_{(k+1)/2}^2 \equiv -bu_{(k-1)/2}^2 \pmod p.$$

Thus,

$$u_{(k+1)/2} \equiv \pm ru_{(k-1)/2} \pmod p.$$

Suppose that $u_{(k+1)/2} \equiv ru_{(k-1)/2} \pmod p$. Then

$$\begin{aligned} u_{(k+3)/2} \equiv au_{(k+1)/2} + bu_{(k-1)/2} &\equiv aru_{(k-1)/2} + bu_{(k-1)/2} \\ &\equiv (ar + b)u_{(k-1)/2} \pmod p. \end{aligned}$$

Now, by (7),

$$\begin{aligned} u_{(k+1)/2}^2 - u_{(k-1)/2}u_{(k+3)/2} &\equiv -bu_{(k-1)/2}^2 - (ar + b)u_{(k-1)/2}^2 \\ &\equiv (-ar - 2b)u_{(k-1)/2}^2 \equiv (-b)^{(k-1)/2} \\ &\equiv r^{k-1} \pmod p. \end{aligned}$$

Since $k - 1$ is even, this implies that $(-2b - ar/p) = 1$.

Now suppose that $u_{(k+1)/2} \equiv -ru_{(k-1)/2} \pmod p$. Continuing as before, we obtain

$$(-2b + ar)u_{(k-1)/2}^2 \equiv r^{k-1} \pmod p.$$

This similarly implies that $(-2b + ar/p) = 1$ and we are done.

In our statement of Lemma 4, note that

$$(-2b + ar)(-2b - ar) = bD.$$

Theorem 10: Consider the PR $u(a, b)$. Let p be an odd prime. Suppose $p \nmid bD$ and $(-b/p) = 1$. Let r be as in Lemma 4.

(i) If $(-b/p) = (bD/p) = 1$ and $(-2b + ar/p) = (-2b - ar/p) = -1$, then, $\alpha(a, b, p) \equiv 0$ or $2 \pmod 4$.

(ii) If $(-b/p) = (bD/p) = (-2b + ar/p) = (-2b - ar/p) = 1$, then $\alpha(a, b, p)$ can be congruent to 0, 1, 2, or 3 (mod 4).

Proof: This follows immediately from Lemma 4.

The following examples in Table 1 from the Fibonacci sequence show the completeness of Theorem 10. For the Fibonacci sequence,

$$a = b = 1,\ D = 5,\ bD = 5,\ -2b + ar = -2 + i, \text{ and } -2b - ar = -2 - i.$$

TABLE 1

Examples from the Fibonacci Sequence in Which $(-b/p) = bD/p) = 1$ and $\alpha(a, b, p)$ Takes on All Possible Values Modulo 4

p	$(-b/p)$	(bD/p)	$(-2b + ar/p)$	$(-2b - ar/p)$	$\alpha(1, 1, p)$ (mod 4)
29	1	1	-1	-1	2
41	1	1	-1	-1	0
61	1	1	1	1	3
421	1	1	1	1	1
809	1	1	1	1	2
1601	1	1	1	1	0

By Theorems 9 and 10, we are so far unable to determine whether the restricted period modulo p is even or odd only when

$$(-b/p) = (bD/p) = (-2b + ar/p) = (-2b - ar/p) = 1.$$

The next theorem will settle this case. We will use the notation $[x/p]_n$ to denote the 2^n - *ic* character of x modulo p.

Theorem 11: Let p be an odd prime and suppose that $p - (D/p) = 2^k q$, where q is an odd integer. Consider the PR $u(a, b)$ and suppose that $p \nmid bD$. Let P be a prime ideal in $K = Q(\sqrt{D})$. Then $\alpha(a, b, p) \equiv 1 \pmod 2$ if and only if

$$r_1^{2q} \equiv (-b)^q \pmod P.$$

If $(D/p) = 1$, then $\alpha(a, b, p) \equiv 1 \pmod 2$ if and only if

$$[r_1/p]_{k-1} \equiv (-b)^q \pmod p.$$

Proof: This is proved by Morgan Ward [13] for the Fibonacci sequence in which case $b = 1$. Our proof will be an immediate generalization of Ward's.

First we note that $u_k \equiv 0 \pmod p$ if and only if

$$r_1^{2k} \equiv (-b)^k \pmod P.$$

This follows from the fact that

$$u_k = r_1^k(r_1^k - r_2^k)/(r_1^k(r_1 - r_2)) = (r_1^{2k} - (r_1 r_2)^k)/(r_1^k(r_1 - r_2))$$
$$= (r_1^{2k} - (-b)^k)/(r_1^k(r_1 - r_2)).$$

The result now follows easily.

Assume that $\alpha(a, b, p) \equiv 1 \pmod 2$. Then, $u_{p-(D/p)} \equiv 0 \pmod p$ by (5). Further, by (6) it follows that $u_m | u_n$ if $m | n$. Thus, $u_q \equiv 0 \pmod p$ since any odd divisor of $p - (D/p)$ must divide q. Thus, by our result earlier in this proof,

$$r_1^{2q} \equiv (-b)^q \pmod P.$$

Conversely, if $r_1^{2q} \equiv 0 \pmod P$, then $u_q \equiv 0 \pmod p$ by the same result. It thus follows that $\alpha(a, b, p) \equiv 1 \pmod 2$. The last remark in the theorem follows from the definition of $[r_1/p]_{k-1}$.

We will generalize the previous theorem in Theorem 12, which will determine when $\alpha(a, b, p) \equiv 2^m \pmod{2^{m+1}}$. First, we will have to prove the following lemma.

Lemma 5: Consider the PR $u(a, b)$. Let p be an odd prime. Suppose that $p \nmid bD$. Let $k = p - (D/p)$. Then

$$p \mid u_{k/2} \text{ iff } (-b/p) = 1.$$

Proof: This was first proved by D. H. Lehmer [4]. Backstrom [1] also gives a proof.

Theorem 12: Consider the PR $u(a, b)$. Let p be an odd prime and suppose that $p - (D/p) = 2^k q$, where q is an odd integer. Suppose $p \nmid bD$. Let P be a prime ideal in K dividing p.

(i) If $(-b/p) = -1$, then $\alpha(a, b, p) \equiv 2^k \pmod{2^{k+1}}$.

(ii) If $(-b/p) = 1$, then $\alpha(a, b, p) \equiv 2^m \pmod{2^{m+1}}$, where $0 < m < k$, if and only if

$$r_1^{2^{m+1}q} \equiv (-b)^{2^m q} \pmod{P}.$$

but

$$r_1^{2^m q} \not\equiv (-b)^{2^{m-1}q} \pmod{P}.$$

(iii) If $(-b/p) = (D/p) = 1$, then $\alpha(a, b, p) \equiv 2^m \pmod{2^{m+1}}$, where $0 < m < k$, if and only if

$$[r_1/p]_{k-m-1} \equiv (-b)^{2^m q} \pmod{p},$$

but

$$[r_1/p]_{k-m} \not\equiv (-b)^{2^{m-1}q} \pmod{p}.$$

Proof:

(i) This follows from Lemma 5, which implies that

$$\alpha(a, b, p) \nmid (p - (D/p))/2.$$

(ii) First, $m < k$, since by Lemma 5,

$$\alpha(a, b, p) \mid (p - (D/p))/2.$$

Further, $\alpha(a, b, p) \equiv 2^m \pmod{2^{m+1}}$ if and only if $p \mid u_{2^m q}$, but $p \nmid u_{2^{m-1}q}$. Now apply the arguments of the preceding theorem, Theorem 11.

(iii) This follows from the definition of the 2^n-*ic* character modulo p and part (ii).

Note, however, that the criteria of Theorems 11 and 12 are not really simpler than direct verification that p is a divisor of some specified term of $\{u_n\}$. For example, in Theorem 11, we can show that $\alpha(a, b, p) \equiv 1 \pmod 2$, if we can show that $p \mid u_q$, where q is the largest odd integer dividing $p - (D/p)$. This is equivalent to the criterion of Theorem 11. In the next section, we will assume that $b = \pm 1$. In this case, the criteria of Theorems 11 and 12 will be easier to apply.

5. THE SPECIAL CASE $b = \pm 1$

In this section we will obtain more complete results than those of Theorems 7 and 8 for those particular PR's for which $b = \pm 1$. We will first treat the case in which $b = 1$ in the following theorems.

Theorem 13: Consider the PR $u(a, 1)$. Let p be an odd prime. Suppose that $(D/p) \neq 0$. If $(-1/p) = 1$, let $i \equiv \sqrt{-1}$, where $0 \leq i \leq (p - 1)/2$.

(i) $\beta(a, 1, p) = 1, 2,$ or 4; $s(a, 1, p) \equiv 1, -1,$ or $\pm i \pmod{p}$.

(ii) $\beta(a, 1, p) = 1$ iff $\alpha(a, 1, p) \equiv 2 \pmod 4$ and $\mu(a, 1, p) \equiv 2 \pmod 4$.

(iii) $\beta(a, 1, p) = 2$ iff $\alpha(a, 1, p) \equiv 0 \pmod 4$ and $\mu(a, 1, p) \equiv 0 \pmod 8$.

(iv) $\beta(a, 1, p) = 4$ iff $\alpha(a, 1, p) \equiv 1 \pmod 2$ and $\mu(a, 1, p) \equiv 4 \pmod 8$.

(v) If $(-1/p) = -1$ and $(a^2 + 4/p) = 1$, then $\alpha(a, 1, p) \equiv 2 \pmod 4$, $\beta(a, 1, p) = 1$, and $\mu(a, 1, p) \equiv 2 \pmod 4$.

(vi) If $(-1/p) = -1$ and $(a^2 + 4/p) = -1$, then $\alpha(a, 1, p) \equiv 0 \pmod 4$, $\beta(a, 1, p) = 2$, and $\mu(a, 1, p) \equiv 0 \pmod 8$.

(vii) If $(-1/p) = 1$ and $(a^2 + 4/p) = -1$, then $\alpha(a, 1, p) \equiv 1 \pmod 2$, $\beta(a, 1, p) = 4$, and $\mu(a, 1, p) \equiv 4 \pmod 8$.

(viii) If $(-1/p) = (a^2 + 4/p) = 1$ and $(-2 + ai/p) = (-2 - ai/p) = -1$, then $\alpha(a, 1, p) \equiv 0$ or $2 \pmod 4$ and $\beta(a, 1, p) = 1$ or 2.

(ix) If $(-1/p) = (a^2 + 4/p) = 1$ and $p \equiv 5 \pmod 8$, then $\alpha(a, 1, p) \not\equiv 0 \pmod 4$ and $\beta(a, 1, p) \neq 2$.

Proof:

(i) Apply Theorem 7. Since $-b = -1$, $\text{ord}_p(-b) = 2$; hence, $H = \alpha(a, 1, p)$ or $H = 2\alpha(a, 1, p)$. Since $\beta(a, 1, p) = H/\alpha(a, 1, p)$ or $\beta(a, 1, p) = 2H/\alpha(a, 1, p)$, $\beta(a, 1, p) = 1$, 2, or 4.

(ii)-(iv) These follow from Theorem 7.

(v)-(vii) These follow from Theorem 9.

(viii) This follows from Theorem 10.

(ix) Suppose $p \equiv 5 \pmod 8$. Then I claim that $\alpha(a, 1, p) \not\equiv 0 \pmod 4$, and, consequently, $\beta(a, 1, p) \neq 2$. Let $k = \alpha(a, 1, p)$, then by part (iii) of this theorem,

$$2k = \mu(a, 1, p) \equiv 0 \pmod 8.$$

Since $(a^2 + 4/p) = (D/p) = 1$, $2k \mid p - 1$ by Theorem 6(i). But then $p \equiv 1 \pmod 8$, which contradicts the fact that $p \equiv 5 \pmod 8$.

Theorem 14: Consider the PR $u(a, 1)$. Let p be an odd prime such that $(-1/p) = (D/p) = 1$. Let $p - 1 = 2^k q$, where q is an odd integer. Let $\varepsilon = (a_0 + c_0\sqrt{D'})/2$ be the fundamental unit in $K = Q(\sqrt{D'})$, where D' is the square-free part of D. Let $\bar{\varepsilon} = -1/\varepsilon$. Consider further the PR $u(a_0, 1)$.

(i) $N(\varepsilon) = -1$, $r_1 = \varepsilon^m$, and $r_2 = -\varepsilon^{-m} = (\bar{\varepsilon})^m$, where $m \equiv 1 \pmod 2$ and r_1 and r_2 correspond to the PR $u(a, 1)$.

(ii) $\alpha(a, 1, p) \mid \alpha(a_0, 1, p)$.

(iii) Either $\alpha(a, 1, p) \equiv \alpha(a_0, 1, p) \equiv 1 \pmod 2$ or $\alpha(a, 1, p) \equiv \alpha(a_0, 1, p) \pmod 4$.

(iv) If $[\varepsilon/p]_{k-1} = -1$, then $\alpha(a, 1, p) \equiv 1 \pmod 2$, $\beta(a, 1, p) = 4$, and $\mu(a, 1, p) \equiv 4 \pmod 8$.

(v) If $[\varepsilon/p]_{k-1} = 1$, then $\alpha(a, 1, p) \equiv 2 \pmod 4$, $\beta(a, 1, p) = 1$, and $\mu(a, 1, p) \equiv 2 \pmod 4$.

(vi) If $[\varepsilon/p]_{k-2} \neq 1$, then $\alpha(a, 1, p) \equiv 0 \pmod 4$, $\beta(a, 1, p) = 2$, and $\mu(a, 1, p) \equiv 0 \pmod 8$.

Proof:

(i) Since $N(r_1) = r_1 r_2 = -1$, it follows that $N(\varepsilon) = -1$, $r_1 = \varepsilon^m$, and $r_2 = -\varepsilon^{-m} = (\bar{\varepsilon})^m$, where $m \equiv 1 \pmod 2$.

(ii) First, we will see that ε and $\bar{\varepsilon}$ are roots of the characteristic polynomial

$$x^2 - a_0 x - 1 = 0$$

associated with the PR $u(a_0, 1)$. Let

$$r_1' = (a_0 + \sqrt{a_0^2 + 4})/2 \quad \text{and} \quad r_2' = (a_0 - \sqrt{a_0^2 + 4})/2$$

be the roots of the characteristic polynomial. By definition of the fundamental unit ε, it is easily seen that

$$a_0^2 - D'c_0^2 = -4.$$

Hence, $\sqrt{a_0^2 + 4} = c_0\sqrt{D'}$. Thus,

$$\varepsilon = (a_0 + c_0\sqrt{D'})/2 = r_1' \quad \text{and} \quad \bar{\varepsilon} = (a_0 - c_0\sqrt{D'})/2 = r_2'.$$

Now, by Theorem 6(ii), $\alpha(a_0, 1, p)$ is the exponent of $\varepsilon/\bar{\varepsilon} = -\varepsilon^2$ modulo p. Similarly, $\alpha(a, 1, p)$ is the exponent of $r_1/r_2 = (-\varepsilon^2)^m$ modulo p. It is now easy to see that

$$\alpha(a, 1, p) = \alpha(a_0, 1, p)/(m, \alpha(a_0, 1, p)). \tag{17}$$

Clearly, $\alpha(a, 1, p) | \alpha(a_0, 1, p)$.

(iii) Since m is odd, it is easy to see from (17) that (iii) holds.

(iv) By definition,

$$[\varepsilon/p]_{k-1} = \varepsilon^{(p-1)/2^{k-1}} = \varepsilon^{2q} \equiv -1 \equiv (-1)^q \pmod{p}.$$

By Theorem 11, it now follows that $\alpha(a_0, 1, p) \equiv 1 \pmod{2}$. By part (iii),

$$\alpha(a, 1, p) \equiv \alpha(a_0, 1, p) \equiv 1 \pmod{2}.$$

The result now follows by Theorem 13(iv).

(v) and (vi) The proofs of these parts are similar to that of part (iv).

The advantage of Theorem 14 is that it gives results for the infinite number of PR's $u(a, 1)$, for which the discriminants D all have the same square-free part D', by analyzing only one PR $u(a_0, 1)$. When the 2^n - *ic* characters modulo p in Theorem 14 are merely the quadratic characters, computations are considerably easier. Further, when D' is a prime, we can make use of several identities to calculate the quadratic characters. The following theorem discusses this in more detail.

Theorem 15: Consider the PR $u(a, 1)$. Suppose that D', the square-free part of D, is an odd prime. Let p be an odd prime. Suppose that

$$(-1/p) = (-1/D') = (p/D') = (D'/p) = 1.$$

Let $\varepsilon_1 = (a_1 + c_1\sqrt{D'})/2$ be the fundamental unit in $K = Q(\sqrt{D'})$.
Let $\varepsilon_2 = (a_2 + c_2\sqrt{p})/2$ be the fundamental unit in $Q(\sqrt{p})$.
Let $D' = m_1^2 + 4n_1^2$ and $p = m_2^2 + 4n_2^2$.
Let $\delta_1 = (m_1 + \sqrt{D'})/2$ and $\delta_2 = (m_2 + \sqrt{p})/2$.
Let $i = \sqrt{-1}$.

(i)
$$\begin{aligned}(\varepsilon_1/p) &= (\delta_1/p) = (m_1 + 2n_1 i/p) = (a_1 + 2i/p) = (m_1 n_2 - m_2 n_1/p)\\ &= (\varepsilon_2/D') = (\delta_2/D') = (m_2 + 2n_2 i/D') = (a_2 + 2i/D')\\ &= (m_1 n_2 - m_2 n_1/D').\end{aligned}$$

(ii) If $(\varepsilon_1/p) = 1$ and $p \equiv 5 \pmod{8}$, then

$$\alpha(a, 1, p) \equiv 2 \pmod{4},\ \beta(a, 1, p) = 1, \text{ and } \mu(a, 1, p) \equiv 2 \pmod{4}.$$

(iii) If $(\varepsilon_1/p) = -1$ and $p \equiv 5 \pmod{8}$, then

$$\alpha(a, 1, p) \equiv 1 \pmod{2},\ \beta(a, 1, p) = 4, \text{ and } \mu(a, 1, p) \equiv 4 \pmod{8}.$$

(iv) If $(\varepsilon_1/p) = -1$ and $p \equiv 1 \pmod{8}$, then

$$\alpha(a, 1, p) \equiv 0 \pmod{4},\ \beta(a, 1, p) = 2, \text{ and } \mu(a, 1, p) \equiv 0 \pmod{8}.$$

(v) If $(\varepsilon_1/p) = 1$ and $p \equiv 9 \pmod{16}$, then

$$\alpha(a, 1, p) \not\equiv 0 \pmod{4},\ \beta(a, 1, p) \neq 2, \text{ and } \mu(a, 1, p) \not\equiv 0 \pmod{8}.$$

Proof:

(i) This is proved by Emma Lehmer in [6].

(ii) This follows from Theorem 14(v).

(iii) This follows from Theorem 14(iv).

(iv) and (v) These follow from Theorem 14(iv)-(vi).

In the case of the Fibonacci sequence, $a = b = 1$ and $D = D' = 5$, which is a prime. Further, the fundamental unit of $Q(\sqrt{5})$ is $\varepsilon_5 = (1 + \sqrt{5})/2$, and 5 can be partitioned as

$$5 = 1^2 + 4(1)^2.$$

With these facts, we can easily apply the criteria of Theorem 15 to the Fibonacci sequence. Wherever possible, we prefer to use the criteria of Theorems 13 and 15, since these involve only quadratic characters rather than the higher-order $2 - ic$ characters used in Theorem 14. Theorems 13 and 15 suffice to determine $\alpha(1, 1, p) \pmod 4$ and, consequently, $\beta(1, 1, p)$ for all odd primes $p <$ 1,000 except $p = 89, 401, 521, 761, 769$, and 809. Further, we know from Theorem 15(v) that none of $\beta(1, 1, 89)$, $\beta(1, 1, 521)$, $\beta(1, 1, 761)$, or $\beta(1, 1, 809)$ are equal to 2.

There are additional rules to determine (ε_5/p) in addition to those of Theorem 15. These are given by Emma Lehmer [5], [6], and [7]. Suppose that $p \equiv 1 \pmod 4$ and $(5/p) = 1$. Then the prime p can be represented as

$$p = m^2 + n^2, \tag{18}$$

where $m \equiv 1 \pmod 4$ and $5|m$ or $5|n$. Another quadratic partition of p is

$$p = c^2 + 5d^2. \tag{19}$$

Further, if we express the fundamental unit of $Q(\sqrt{p})$ as $(f + g\sqrt{p})/2$, then either $5|f$ or $5|g$. We then have the following criteria for determining (ε_5/p):

$$(\varepsilon_5/p) = 1 \text{ iff } p \equiv 1 \pmod{20} \text{ and } n \equiv 0 \pmod 5, \text{ or } p \equiv 9 \pmod{20} \text{ and } m \equiv 0 \pmod 5. \tag{20}$$

$$(\varepsilon_5/p) = (-1)^d. \tag{21}$$

$$(\varepsilon_5/p) = 1 \text{ iff } f \equiv 0 \pmod 5. \tag{22}$$

Now, suppose that p and q are both odd primes and that $(-1/p) = (-1/q) = (p/q) = (q/p) = 1$. Let ε_q be the fundamental unit of $Q(\ p)$. Emma Lehmer [7] has given an analogous rule to that of equation (21) to determine (ε_q/p) in terms of the representability of p or $2p$ by the form

$$c^2 + qd^2$$

in the cases $q = 13, 17, 37, 41, 73, 97, 113, 137, 193, 313, 337, 457$, and 577. These results are applicable to Theorem 15 when $D' = q$.

We now treat the PR's for which $b = -1$ and $|a| \geq 3$. The PR's $u(a, -1)$ for which $|a| \leq 2$ are treated in Theorem 4.

Theorem 16: Consider the PR $u(a, -1)$. Let p be an odd prime. Suppose $p \nmid D$.

(i) $\beta(a, -1, p) = 1$ or 2; $s(a, -1, p) \equiv 1$ or $-1 \pmod p$.

(ii) If $\alpha(a, -1, p) \equiv 0 \pmod 2$, then $\beta(a, -1, p) = 2$ and $\mu(a, -1, p) \equiv 0 \pmod 4$.

(iii) If $\alpha(a, -1, p) \equiv 1 \pmod 2$, then $\beta(a, -1, p)$ may be 1 or 2, and $\mu(a, -1, p)$ may be congruent to $1 \pmod 2$ or $2 \pmod 4$.

(iv) If $(2 - a/p) = (2 + a/p) = -1$, then

$$\alpha(a, -1, p) \equiv 0 \pmod 2,\ \beta(a, -1, p) = 2, \text{ and } \mu(a, -1, p) \equiv 0 \pmod 4.$$

(v) If $(2 - a/p) = 1$ and $(2 + a/p) = -1$, then

$$\alpha(a, -1, p) \equiv 1 \pmod 2,\ \beta(a, -1, p) = 2, \text{ and } \mu(a, -1, p) \equiv 2 \pmod 4.$$

(vi) If $(2 - a/p) = -1$ and $(2 + a/p) = 1$, then

$$\alpha(a, -1, p) \equiv 1 \pmod 2,\ \beta(a, -1, p) = 1, \text{ and } \mu(a, -1, p) \equiv 1 \pmod 2.$$

Proof:

(i) By Theorem 7,

$$\beta(a, -1, p) = H/\alpha(a, -1, p) \quad \text{or} \quad \beta(a, -1, p) = 2H/\alpha(a, -1, p).$$

Since $-b = 1$, $\mathrm{ord}_p(-b) = 1$, and $H = \alpha(a, -1, p)$. Thus, $\beta(a, -1, p) = 1$ or 2.

(ii) and (iii) These follow from Theorem 7 and the comment following Theorem 7.

(iv) This follows from part (ii) and Theorem 10(i).

(v) and (vi) First notice that in both cases,

$$(4 - a^2/p) = -1 = (bD/p).$$

Thus, by Theorem 9(i), $\alpha(a, -1, p) \equiv 1 \pmod 2$. Now, let $k = \alpha(a, -1, p) \equiv 1 \pmod 2$. Then, by (6),

$$u_k = -u^2_{(k-1)/2} + u^2_{(k+1)/2} \equiv 0 \pmod p. \tag{23}$$

Hence,

$$u_{(k+1)/2} \equiv \pm u_{(k-1)/2} \pmod p.$$

First, suppose that $u_{(k+1)/2} \equiv u_{(k-1)/2} \pmod p$. Then,

$$u_{(k+3)/2} = -u_{(k-1)/2} + au_{(k+1)/2} \equiv (a-1)u_{(k+1)/2} \pmod p.$$

Then, by (7),

$$\begin{aligned} u^2_{(k+1)/2} - u_{(k+3)/2} \cdot u_{(k-1)/2} &\equiv u^2_{(k+1)/2} - (a-1)u^2_{(k+1)/2} \\ &\equiv (2-a)u^2_{(k+1)/2} \equiv 1^{(k-1)/2} \equiv 1 \pmod p. \end{aligned}$$

Thus, $u^2_{(k+1)/2} \equiv 1/(2-a) \pmod p$, and $(2 - a/p) = 1$. Now, by (6),

$$\begin{aligned} u_{k+1} &= -u_{(k+1)/2} \cdot u_{(k-1)/2} + u_{(k+1)/2} \cdot u_{(k+3)/2} \\ &\equiv -u^2_{(k+1)/2} + (a-1)u^2_{(k+1)/2} \equiv (a-2)u^2_{(k+1)/2} \\ &\equiv (a-2)/(2-a) \equiv -1 \pmod p. \end{aligned}$$

Thus, if $\alpha(a, -1, p) \equiv 1 \pmod 2$ and $u_{(k+1)/2} \equiv u_{(k-1)/2} \pmod p$, then,

$$(2 - a/p) = 1 \quad \text{and} \quad \beta(a, -1, p) = 2.$$

Now, suppose that $u_{(k+1)/2} \equiv -u_{(k-1)/2} \pmod p$. Then,

$$u_{(k+3)/2} = -u_{(k-1)/2} + au_{(k+1)/2} \equiv (a+1)u_{(k+1)/2} \pmod p.$$

Further,

$$u^2_{(k+1)/2} - u_{(k-1)/2} \cdot u_{(k+3)/2} \equiv (a+2)u^2_{(k+1)/2} \equiv 1^{(k-1)/2} \equiv 1 \pmod p.$$

Then, $u^2_{(k+1)/2} \equiv 1/(2+a) \pmod p$, and $(2 + a/p) = 1$. Now,

$$\begin{aligned} u_{k+1} &= -u_{(k+1)/2} \cdot u_{(k-1)/2} + u_{(k+1)/2} \cdot u_{(k+3)/2} \equiv (a+2)u^2_{(k+1)/2} \\ &\equiv (a+2)/(a+2) \equiv 1 \pmod p. \end{aligned}$$

Hence, if $(a, -1, p) \equiv 1 \pmod 2$ and $u_{(k+1)/2} \equiv -u_{(k-1)/2} \pmod p$, then,

$$(2 + a/p) = 1 \quad \text{and} \quad \beta(a, -1, p) = 1.$$

Parts (v) and (vi) now follow immediately.

Theorem 17: Consider the PR $u(a, -1)$, where $|a| \geq 3$. Let p be an odd prime such that $(4 - a^2/p) = (2 - a/p) = (2 + a/p) = 1$. Let $\varepsilon = (a_0 + c_0\sqrt{D'})/2$ be the fundamental unit of $Q(\sqrt{D'})$. Suppose $N(\varepsilon) = -1$. Consider the PR $u(a_0, 1)$. Suppose $\alpha(a_0, 1, p) = 2^k q$, where $q \equiv 1 \pmod 2$.

(i) $r_1 = (a + \sqrt{D})/2 = \varepsilon^m$, where $m = 2^c d$, $c \geq 1$, and $d \equiv 1 \pmod 2$.

(ii) $\alpha(a, -1, p) | \alpha(a_0, 1, p)$.

(iii) If $k = c$, then $(a, -1, p) \equiv 1 \pmod 2$ and

$$s(a, -1, p) \equiv s(a_0, 1, p) \pmod p.$$

Further,

$$\beta(a, -1, p) = 1 \text{ if } \alpha(a_0, 1, p) \equiv 2 \pmod 4.$$

Moreover,

$$\beta(a, -1, p) = 2 \text{ if } \alpha(a_0, 1, p) \equiv 0 \pmod 4.$$

(iv) If $k > c$, then $\alpha(a, -1, p) \equiv 0 \pmod 2$ and $\beta(a, -1, p) = 2$.

(v) If $k < c$, then $\alpha(a, -1, p) \equiv 1 \pmod 2$. If $k = 0$ and $c = 1$, then $\beta(a, -1, p) = 2$. If $c \neq 1$ and $k < c$, then $\beta(a, -1, p) = 1$.

Proof:

(i) Since $N(\varepsilon) = -1$, where ε is the fundamental unit, and

$$N(r_1) = r_1 r_2 = -b = 1,$$

it follows that $r_1 = \varepsilon^m$ where m is even.

(ii) Just as in the proof of Theorem 14(ii), we see that ε and $\bar{\varepsilon}$ are the roots of the characteristic polynomial of the PR $u(a_0, 1)$. Again, just as in equation (17) of the proof of Theorem 14(ii), it follows that

$$\alpha(a, -1, p) = \alpha(a_0, 1, p)/(m, \alpha(a_0, 1, p)). \tag{24}$$

Clearly, $\alpha(a, -1, p) \mid \alpha(a_0, 1, p)$.

(iii) Since m and $\alpha(a_0, 1, p)$ are both even and divisible by the same power of 2, it follows from equation (24) that $\alpha(a, -1, p) \equiv 1 \pmod 2$. Since $\alpha(a_0, 1, p) \equiv 0 \pmod 2$, it follows from Theorem 13 that $s(a_0, 1, p) \equiv \pm 1 \pmod p$. Now, by Theorem 6(iii),

$$s(a_0, 1, p) \equiv \varepsilon^{\alpha(a_0, 1, p)} \equiv \pm 1 \pmod p. \tag{25}$$

Also, by Theorem 6(iii),

$$s(a, -1, p) \equiv (r_1)^{\alpha(a, -1, p)} \equiv (\varepsilon^m)^{\alpha(a_0, 1, p)/(m, \alpha(a_0, 1, p))} \pmod p. \tag{26}$$

The last congruence follows by equation (24) in the proof of part (ii). However, since the same power of 2 divides both m and $\alpha(a_0, 1, p)$, it follows that

$$m/(m, \alpha(a_0, 1, p)) = r,$$

where $r \equiv 1 \pmod 2$. Hence,

$$s(a, -1, p) \equiv [\varepsilon^{\alpha(a_0, 1, p)}]^r \equiv [s(a_0, 1, p)]^r \equiv (\pm 1)^r$$
$$\equiv \pm 1 \equiv s(a_0, 1, p) \pmod p.$$

Since $s(a, -1, p) \equiv s(a_0, 1, p)$, $\beta(a, -1, p) = \beta(a_0, 1, p)$. If $\alpha(a_0, 1, p) \equiv 2 \pmod 4$, then $\beta(a_0, 1, p) = 1$ by Theorem 13(ii). Consequently, $\beta(a, -1, p) = 1$. If $\alpha(a_0, 1, p) \equiv 0 \pmod 4$, then $\beta(a_0, 1, p) = 2 = \beta(a, -1, p)$ by Theorem 13(iii).

(iv) If $k > c$, it follows from equation (24) that $\alpha(a, -1, p) \equiv 0 \pmod 2$. The result now follows from Theorem 16(ii).

(v) If $k < c$, it follows from equation (24) that $\alpha(a, -1, p) \equiv 1 \pmod 2$. By (25) and (26),

$$s(a, -1, p) \equiv [\varepsilon^{\alpha(a_0, 1, p)}]^{m/(m, \alpha(a_0, 1, p))}. \tag{27}$$

If $k = 0$ and $c = 1$, then $\varepsilon^{\alpha(a_0, 1, p)} \equiv \pm\sqrt{-1} \pmod p$ and $\alpha(a_0, 1, p) = 4$ by Theorem 13(iv). Further,

$$m/(m, \alpha(a_0, 1, p)) \equiv 2 \pmod 4,$$

since $k = 0$ and $c = 1$. Thus, by (27),

$$s(a, -1, p) \equiv (\pm\sqrt{-1})^2 \equiv -1 \pmod p,$$

and hence $\beta(a, -1, p) = 2$.

Now, suppose $c \neq 1$ and $k < c$. If $k = 0$, then $c \geq 2$ and

$$4 | m/(m, \alpha(a_0, 1, p)).$$

Then, again, $\varepsilon^{\alpha(a_0, 1, p)} \equiv \pm\sqrt{-1} \pmod{p}$, and by (27),

$$s(a, -1, p) \equiv [\varepsilon^{\alpha(a_0, 1, p)}]^{m/(m, \alpha(a_0, 1, p))} \equiv (\pm\sqrt{-1})^4 \equiv 1 \pmod{p}.$$

Thus, $\beta(a, -1, p) = 1$. If $k \neq 0$ and $k < c$, then,

$$2 | m/(m, \alpha(a_0, 1, p)).$$

Further, by Theorem 13 and Theorem 6(iii),

$$\varepsilon^{\alpha(a_0, 1, p)} \equiv \pm 1 \pmod{p}.$$

Thus, by (27),

$$s(a, -1, p) \equiv [\varepsilon^{\alpha(a_0, 1, p)}]^{m/(m, \alpha(a_0, 1, p))} \equiv (\pm 1)^2 \equiv 1 \pmod{p}.$$

Therefore, $\beta(a_0, 1, p) = 1$, and we are done.

Note that in Theorem 17 we obtain results for the infinite number of PR's $u(a, -1)$ which have the same square-free part of the discriminant D' by considering only one PR $u(a_0, 1)$. Since $b = 1$ for this PR, we are able to make use of Theorems 13-15. Further, note that in Theorem 17 we are able to calculate the exponent k for which $\alpha(a_0, 1, p) \equiv 2^k \pmod{2^{k+1}}$ by Theorem 12. In Theorem 18, we will consider the remaining case where $N(\varepsilon) = 1$.

Theorem 18: Consider the PR $u(a, -1)$. Let p be an odd prime such that

$$(4 - a^2/p) = (2 - a/p) = (2 + a/p) = 1.$$

Let $\varepsilon = (a_0 + c_0\sqrt{D'})/2$ be the fundamental of $Q(\sqrt{D'})$. Suppose that $N(\varepsilon) = 1$. Consider the PR $u(a_0, -1)$. Suppose that $\alpha(a_0, -1, p) = 2^k q$, where $q \equiv 1 \pmod{2}$.

(i) $r_1 = (a + \sqrt{D})/2 = \varepsilon^m$, where $m = 2^c d$, $c \geq 0$, and $d \equiv 1 \pmod{2}$.

(ii) $\alpha(a, -1, p) | \alpha(a_0, -1, p)$.

(iii) If $k = c$ and $k \geq 1$, then $\alpha(a, -1, p) \equiv 1 \pmod{2}$ and $\beta(a, -1, p) = 2$.

(iv) If $k = c = 0$, then $\alpha(a, -1, p) \equiv 1 \pmod{2}$. If

$$s(a_0, -1, p) = \varepsilon^{2^k q} \equiv 1 \pmod{p},$$

then $\beta(a, -1, p) = 1$; otherwise, $\beta(a, -1, p) = 2$.

(v) If $k > c$, then $\alpha(a, -1, p) \equiv 0 \pmod{2}$ and $\beta(a, -1, p) = 2$.

(vi) If $k < c$, then $\alpha(a, -1, p) \equiv 1 \pmod{2}$ and $\beta(a, -1, p) = 1$.

Proof:

(i) This follows since $N(r_1) = r_1 r_2 = 1$ and ε is the fundamental unit of $Q(\sqrt{D'})$.

(ii) It is easy to see that ε and $\bar{\varepsilon}$ are the roots of the characteristic polynomial

$$x^2 - a_0 x + 1 = 0$$

of the PR $u(a_0, -1)$. The rest of the proof follows as in the proofs of Theorem 14(ii) and Theorem 17(ii).

(iii) Just as in the proof of Theorem 17(ii), it follows that

$$\alpha(a, -1, p) = \alpha(a_0, -1, p)/(m, \alpha(a_0, -1, p)). \tag{28}$$

Since $k = c$, it follows that $\alpha(a, -1, p) \equiv 1 \pmod{2}$. Since $\alpha(a_0, -1, p) \equiv 0 \pmod{2}$, it follows from Theorem 13(ii) that $\beta(a_0, -1, p) = 2$ and $s(a_0, -1, p) \equiv -1 \pmod{p}$. By (25) and (26), it follows that

(29) $$s(a, -1, p) \equiv s(a_0, -1, p)^{m/(m, \alpha(a_0, 1, p))}$$
$$\equiv -1^{m/(m, \alpha(a_0, 1, p))} \equiv -1 \pmod{p},$$

since $k = c$. Thus, $\beta(a, -1, p) = 2$.

(iv) It follows just as in the proof of part (iii) that $\alpha(a, -1, p) \equiv 1 \pmod{2}$. By (29),

$$s(a, -1, p) \equiv s(a_0, -1, p)^{m/(m, \alpha(a_0, 1, p))}.$$

Since $k = c$ and $s(a_0, -1, p) \equiv \pm 1 \pmod{p}$ by Theorem 16, it follows that

$$s(a_0, -1, p) \equiv s(a_0, -1, p) \pmod{p}.$$

The rest follows from Theorem 6(iii).

(v) If $k > c$, it follows from (28) that $\alpha(a, -1, p) \equiv 0 \pmod{2}$. It now follows from Theorem 16(ii) that $\beta(a, -1, p) = 2$.

(vi) If $k < c$, it follows from (28) that $\alpha(a, -1, p) \equiv 1 \pmod{2}$. By (29),

$$s(a, -1, p) \equiv s(a_0, -1, p)^{m/(m, \alpha(a_0, 1, p))}.$$

Since $k < c$, $m/(m, \alpha(a_0, -1, p)) \equiv 0 \pmod{2}$. Since $s(a_0, -1, p) \equiv \pm 1 \pmod{p}$, it now follows that

$$s(a, -1, p) \equiv (\pm 1)^2 \equiv 1 \pmod{p}.$$

Thus, $\beta(a, -1, p) = 1$.

In Theorem 18, we are again able to calculate the exponent k for which $\alpha(a_0, -1, p) \equiv 2^k \pmod{2^{k+1}}$ by Theorem 12. Theorem 18 just reduces the problem of finding the restricted period modulo p of a PR $u(a, -1)$ for which $b = -1$ to that of considering another PR $u(a_0, -1)$ for which also $b = -1$. However, since $r_1 = \varepsilon^m$, $|a_0| \leq |a|$, and it is easier to work with the PR $u(a_0, -1)$ instead of the PR $u(a, -1)$.

6. THE SPECIAL CASE $r_2 = \pm 1$

In this section, we will conclude our paper by considering those PR's for which one of the characteristic roots is ± 1. Theorems 19 and 20 will treat these cases.

Theorem 19: Consider the PR $u(-b + 1, b)$, where $b \neq 0$ and $b \neq 1$. Then $r_1 = -b$, $r_2 = 1$, and $D = (b + 1)^2$. Let p be an odd prime such that $b \not\equiv 0$ and $b \not\equiv -1 \pmod{p}$. If $(-b/p) = 1$, let $r^2 \equiv -b \pmod{p}$, where $0 \leq r \leq (p - 1)/2$.

(i) $\alpha(-b + 1, b, p) = \text{ord}_p(-b)$.

(ii) $\beta(-b + 1, b, p) = 1$ always; $s(-b + 1, b, p) \equiv 1 \pmod{p}$ always.

(iii) If $(-b/p) = -1$ and $p \equiv 3 \pmod{4}$, then

$$\alpha(-b + 1, b, p) = \mu(-b + 1, b, p) \equiv 2 \pmod{4}.$$

(iv) If $(-b/p) = -1$ and $p \equiv 1 \pmod{4}$, then

$$\alpha(-b + 1, b, p) = \mu(-b + 1, b, p) \equiv 0 \pmod{4}.$$

(v) If $(-b/p) = 1$ and $p \equiv 3 \pmod{4}$, then

$$\alpha(-b + 1, b, p) = \mu(-b + 1, b, p) \equiv 1 \pmod{2}.$$

(vi) If $(-b/p) = 1$, $p \equiv 1 \pmod{4}$, and

$$(-2b + (1 - b)r/p) = (-2b - (1 - b)r/p) = -1,$$

then $\alpha(-b + 1, b, p)$ is congruent to 0 or 2 modulo 4.

(vii) Suppose that $p - 1 = 2^k q$, where $q \equiv 1 \pmod{2}$. If $(-b/p) = -1$, then $\alpha(-b + 1, b, p) \equiv 2^k \pmod{2^{k+1}}$. If $(-b/p) = 1$, then $\alpha(-b + 1, b, p) \equiv 2^m \pmod{2^{m+1}}$, where $0 < m < k$ iff

$$[-b/p]_{k-m} \equiv 1 \pmod{p}, \text{ but } [-b/p]_{k-m+1} \equiv -1 \pmod{p}.$$

Further,

$$\alpha(-b+1, b, p) \equiv 1 \pmod{2} \text{ iff } [-b/p]_k \equiv 1 \pmod{p}.$$

Proof:

(i) and (ii) Since $a = -b + 1$, it easily follows that $r_1 = -b$ and $r_2 = 1$. By Theorem 6(ii), it follows that

$$\mu(-b+1, b, p) = \text{ord}_p(r_1/r_2) = \text{ord}_p(-b).$$

Further, by Theorem 6(i),

$$(-b+1, b, p) = [\text{ord}_p(-b), \text{ord}_p(1)] = \text{ord}_p(-b).$$

The results now follow.

(iii)-(vi) These follow from Theorems 9 and 10.

(vii) This follows from Theorem 12 and Theorem 11.

Theorem 20: Consider the PR $u(b-1, b)$, where $b \neq 0$ and $b \neq -1$. Then $r_1 = b$, $r_2 = -1$, and $D = (b+1)^2$. Let p be an odd prime such that $b \not\equiv 0$ and $b \not\equiv -1 \pmod{p}$. Suppose $p = 2^k q$, where $k \equiv 1 \pmod{2}$. If $(-b/p) = 1$, let $r^2 \equiv -b \pmod{p}$, where $0 \leq r \leq (p-1)/2$.

(i) $\alpha(b-1, b, p) = \text{ord}_p(-b)$.

(ii) $\beta(b-1, b, p) = 1$ or 2; $s(b-1, b, p) \equiv \pm 1 \pmod{p}$.

(iii) If $\alpha(b-1, b, p) \equiv 1 \pmod{2}$, then $\beta(b-1, b, p) = 2$.
If $\alpha(b-1, b, p) \equiv 0 \pmod{2}$, then $\beta(b-1, b, p) = 1$.

(iv) If $(-b/p) = -1$ and $p \equiv 3 \pmod{4}$, then

$$\alpha(b-1, b, p) = \mu(b-1, b, p) \equiv 2 \pmod{4}.$$

(v) If $(-b/p) = -1$ and $p \equiv 1 \pmod{4}$, then

$$\alpha(b-1, b, p) = \mu(b-1, b, p) \equiv 0 \pmod{4}.$$

(vi) If $(-b/p) = 1$ and $p \equiv 3 \pmod{4}$, then

$$\alpha(b-1, b, p) \equiv 1 \pmod{2} \text{ and } \mu(b-1, b, p) \equiv 2 \pmod{4}.$$

Hence, if $p \equiv 3 \pmod{4}$, then $\mu(b-1, b, p) \equiv 2 \pmod{4}$.

(vii) If $(-b/p) = 1$, $p \equiv 1 \pmod{4}$, and

$$(-2b + (b-1)r/p) = (-2b - (b-1)r/p) = -1,$$

then $\alpha(b-1, b, p)$ is congruent to 0 or 2 (mod 4).

(viii) If $(-b/p) = -1$, then $\alpha(b-1, b, p) \equiv 2^k \pmod{2^{k+1}}$.
If $(-b/p) = 1$, then $\alpha(b-1, b, p) \equiv 2^m \pmod{2^{m+1}}$, where $0 < m < k$ iff

$$[-b/p]_{k-m} \equiv 1 \pmod{p}, \text{ but } [-b/p]_{k-m+1} \equiv -1 \pmod{p}.$$

Further, $\alpha(b-1, b, p) \equiv 1 \pmod{2}$ iff $[-b/p]_k \equiv 1 \pmod{p}$.

Proof:

(i)-(iii) If $a = b - 1$, it follows that $r_1 = b$ and $r_2 = -1$. Now, by Theorem 6(i),

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

If $\text{ord}_p(b) \equiv 0 \pmod{4}$, then $\text{ord}_p(b) = \text{ord}_p(-b) = \mu(b-1, b, p)$.

If $\text{ord}_p(b) \equiv 2 \pmod{4}$, then $\text{ord}_p(-b) \equiv 1 \pmod{2}$.

Thus,

$$\text{ord}_p(b) = \mu(b-1, b, p) = 2 \cdot \text{ord}_p(-b).$$

If $\text{ord}_p(b) \equiv 1 \pmod{2}$, then $\text{ord}_p(-b) \equiv 2 \pmod{4}$.

Hence,

$$\text{ord}_p(-b) = 2 \cdot \text{ord}_p(b) = \mu(b-1, b, p).$$

Now, by Theorem 6(ii),

$$\alpha(b-1, b, p) = \text{ord}_p(r_1/r_2) = \text{ord}_p(-b).$$

Thus, by our above argument, if $\alpha(b - 1, b, p) \equiv 0 \pmod 2$, then

$$\alpha(b - 1, b, p) = \mu(b - 1, b, p), \text{ and } \beta(b - 1, b, p) = 1.$$

If $\alpha(b - 1, b, p) \equiv 1 \pmod 2$, then

$$\mu(b - 1, b, p) = 2\alpha(b - 1, b, p), \text{ and } \beta(b - 1, b, p) = 2.$$

The results of parts (i)-(iii) now follows.

(iv)-(vii) These follow from Theorems 9 and 10.

(viii) This follows from Theorems 11 and 12.

REFERENCES

1. Robert P. Backstrom. "On the Determination of the Zeros of the Fibonacci Sequence." *The Fibonacci Quarterly* 4, No. 4 (1966):313-322.
2. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n + \beta^n$." *Annals of Mathematics*, 2nd Ser. 15 (1913):30-70.
3. John H. Halton. "On the Divisibility Properties of Fibonacci Numbers." *The Fibonacci Quarterly* 4, No. 3 (1966):217-240.
4. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Annals of Mathematics*, 2nd Ser. 31 (1930):419-448.
5. Emma Lehmer. "On the Quadratic Character of the Fibonacci Root." *The Fibonacci Quarterly* 4, No. 2 (1966):135-138.
6. Emma Lehmer. "On the Quadratic Character of Some Quadratic Surds." *Journal für die Reine und Angewandte Mathematik* 250 (1971):42-48.
7. Emma Lehmer. "On Some Special Quartic Reciprocity Laws." *Acta Arithmetica* 21 (1972):367-377.
8. Edouard Lucas. "Théorie des fonctions numériques simplement périodiques." *American Journal of Mathematics* 1 (1878):184-240, 289-321.
9. D. W. Robinson. "The Fibonacci Matrix Modulo *m*." *The Fibonacci Quarterly* 1, No. 1 (1963):29-36.
10. Lawrence Somer. "Which Second-Order Recurrences Have Almost All Primes as Divisors?" *The Fibonacci Quarterly* 17, No. 2 (1979):111-116.
11. John Vinson. "The Relation of the Period Modulo *m* to the Rank of Apparition of *m* in the Fibonacci Sequence." *The Fibonacci Quarterly* 1, No. 1 (1963):37-45.
12. D. D. Wall. "Fibonacci Series Modulo *m*." *American Mathematical Monthly* 67 (1960):525-532.
13. Morgan Ward. "The Prime Divisors of Fibonacci Numbers." *Pacific Journal of Mathematics* 11 (1961):379-386.
14. O. Wyler. "On Second-Order Recurrences." *American Mathematical Monthly* 72 (1965):500-506.

*****

MIXING PROPERTIES OF MIXED CHEBYSHEV POLYNOMIALS

CLARK KIMBERLING

University of Evansville, Evansville, Indiana 47702

The *Chebyshev polynomials of the first kind*, defined recursively by

$$t_0(x) = 1,\ t_1(x) = x,\ t_n(x) = 2xt_{n-1}(x) - t_{n-2}(x) \text{ for } n = 2, 3, \ldots,$$

or equivalently, by

$$t_n(x) = \cos(n \cos^{-1} x) \text{ for } n = 0, 1, \ldots,$$

commute with one another under composition; that is

$$t_m(t_n(x)) = t_n(t_m(x)).$$