DIVISIBILITY PROPERTIES OF CERTAIN RECURRING SEQUENCES

RONALD SOLOMON
Department of Mathematics, Ohio State University, Columbus, Ohio 43210

We shall consider the sequences, $\{w_n(r,s;a,c)\}$, defined by $w_0 = r$, $w_1 = s$ and $w_n = aw_{n-1} + cw_{n-2}$ for $n \geqslant 2$; henceforth denoted by $\{w_n\}$ where no ambiguity may result. We shall confine our attention to those sequences for which $r, s, a,$ and c are integers with $(a,c) = 1$, $(r,s) = 1$, $(s,c) = 1$, $ac \neq 0$ and $w_n \neq 0$ for $n \geqslant 1$. The major result of this paper will be a complete classification of all sequences $\{w_n\}$ for which $w_k \mid w_{2k}$ for all integers $k \geqslant 1$.

If $w_0 = 0$ and $w_1 = 1$, we have a well known sequence which we shall denote, following Carmichael [1], by $\{D_n(a,c)\}$, or $\{D_n\}$ if no ambiguity may result, and concerning which we shall assume the following facts to be known (cf. [1], [2]):

F1: $(D_n, c) = 1$ for all $n \geqslant 1$,

F2: $(D_n, D_{n+1}) = 1$ for all n.

F3: If c is even, then D_n is odd for all n.
If c is odd and a is even, then $D_n \equiv n \pmod 2$ for all n.
If both a and c are odd, then D_n is even if and only if $n \equiv 0 \pmod 3$.

F4: Let $b = a^2 + 4c$ and let p be an odd prime.
Let $(b/p) = \begin{cases} (b/p) & \text{if } (b,p) = 1 \\ 0 & \text{if } p \mid b. \end{cases}$
If $(p,c) = 1$, then $p \mid D_p - (b/p)$.

F5: $D_{m+n} = cD_mD_{n-1} + D_{m+1}D_n$ for all $m \geqslant 0$ and $n \geqslant 1$.

F6: If $m \mid n$, then $D_m \mid D_n$.

If $w_0 = 2$ and $w_1 = a$, we have a well known sequence which we shall denote, following Carmichael [1], by $\{S_n(a,c)\}$,* or by $\{S_n\}$ if no ambiguity may result, and concerning which we assume the following fact to be known:

F7: $D_{2n} = D_nS_n$ for all n.

Theorem 1: $w_n(r,s;a,c) = sD_n(a,c) + rcD_{n-1}(a,c)$ for all $n \geqslant 1$.

The proof is by complete mathematical induction on n:

1. $sD_1 + rcD_0 = s = w_1$.
2. $sD_2 + rcD_1 = as + rc = w_2$
3. Suppose the theorem is true for all n less than some fixed integer $k \geqslant 3$. Then $w_{k-1} = sD_{k-1} + rcD_{k-2}$ and

$$w_{k-2} = sD_{k-2} + rcD_{k-3}.$$

So

*We differ from Carmichael in requiring that $(a,2) = 1$. If $(a,2) = 2$, $w_n(1, (a/2); a,c) = \tfrac{1}{2}S_n(a,c)$ for all n, and hence the former sequence has essentially the same divisibility properties as the latter.

$$w_k = a(sD_{k-1} + rcD_{k-2}) + c(sD_{k-2} + rcD_{k-3}) = s(aD_{k-1} + cD_{k-2}) + rc(aD_{k-2} + cD_{k-3}) = sD_k + rcD_{k-1}.$$

Using (F1), (F2) and the fact that $(r,s) = 1$, we have:

Corollary: $(w_n, D_n) = (r, D_n) = (r, w_n)$, $(w_n, D_{n-1}) = (s, D_{n-1}) = (s, w_n)$.

Theorem 2: $(w_n, w_{n+1}) = 1$ for all $n \geq 0$.

The proof is by induction on n:

1. $(w_0, w_1) = (r, s) = 1$.
2. $(w_1, w_2) = (s, as + cr) = (s, cr) = 1$.
3. Suppose $(w_{k-1}, w_k) = 1$ for some fixed integer $k \geq 2$. Let $(w_k, w_{k+1}) = d$. Since $w_{k+1} = aw_k + cw_{k-1}$, $d | cw_{k-1}$, whence $d|c$. Now $w_k = aw_{k-1} + cw_{k-2}$, whence $d|n$. Hence $d = 1$.

Theorem 3: $(w_n, c) = 1$ for all $n \geq 1$.

Proof:

1. $(w_1, c) = (s, c) = 1$.
2. Suppose $n \geq 2$. Then $w_n = aw_{n-1} + cw_{n-2}$. Let $d = (w_n, c)$. Then $d | aw_{n-1}$. Hence, by Theorem 2, $d = 1$.

Theorem 4. (a) If c is even, then w_n is odd for all $n \geq 1$.

(b) If a is even and c is odd, then
  (i) If n is odd, then $w_n \equiv s \pmod 2$.
  (ii) If n is even, then $w_n \equiv r \pmod 2$.

(c) If a and c are both odd, then
  (i) If $n \equiv 0 \pmod 3$, then $w_n \equiv r \pmod 2$.
  (ii) If $n \equiv 1 \pmod 3$, then $w_n \equiv s \pmod 2$.
  (iii) If $n \equiv 2 \pmod 3$, then $w_n \equiv r + s \pmod 2$.

Proof: Part (a) is immediate from Theorem 3.
Parts (b) and (c) follow from (F3) and Theorem 1.

Corollary: If r is even, then $w_n \equiv D_n \pmod 2$ for all n.

Theorem 5: Let p be any odd prime.

(a) If $p|c$, then $(p, w_n) = 1$ for all $n \geq 1$.
(b) If $(p,c) = 1$, then $p | w_{p-(b/p)}$ if and only if $p|r$.

Proof: Part (a) is immediate from Theorem 3.
Part (b) follows from (F4) and Theorem 1.

REMARK: The only recurring sequences for which $p | w_{p-(b/p)}$ for more than a finite number of primes p are $\pm\ D_n(a,c)$.

Theorem 6: $w_{m+n} = cD_{n-1}w_m + D_n w_{m+1}$ for all $m \geq 0$ and $n \geq 1$.

Proof:

$$w_{m+n} = sD_{m+n} + rcD_{m+n-1} \quad \text{(by Theorem 1)};$$
$$= s(cD_mD_{n-1} + D_{m+1}D_n) + rc(cD_{m-1}D_{n-1} + D_mD_n) \quad \text{(by F5)};$$
$$= cD_{n-1}(sD_m + rcD_{m-1}) + D_n(sD_{m+1} + rcD_m)$$
$$= cD_{n-1}w_m + D_n w_{m+1} \quad \text{(by Theorem 1)}.$$

Corollary 1: $(w_n, w_k) = (w_n, D_{n-k}) = (w_k, D_{n-k})$, where $n \geq k \geq 0$.

Proof: This corollary is immediate if $n = k$. Suppose $n \geq k \geq 0$. Then

$$w_n = w_{k+(n-k)} = cD_{n-k-1}w_k + D_{n-k}w_{k+1}.$$

Hence if $d|w_n$ and $d|w_k$, then $d|D_{n-k}w_{k+1}$. By Theorem 2, $(w_k, w_{k+1}) = 1$. Hence $d|D_{n-k}$.
Similarly, if $d|w_n$ and $d|D_{b-k}$, then $d|cD_{n-k-1}w_k$. But $(D_{n-k}, dD_{n-k-1}) = 1$. So $d|w_k$.
Finally, if $d|w_k$ and $d|D_{n-k}$, then $d|w_n$.

Corollary 2: $w_k | w_n$ if and only if $w_k | D_{n-k}$, where $n \geq k \geq 1$.

Corollary 2: $w_k | w_n$ if and only if $w_k | D_{n-k}$, where $n \geq k \geq 1$.

Corollary 3: (a) $w_k | w_{mk}$ if and only if $w_k | D_{(m-1)k}$ for $n \geq 1$.

(b) If $w_k | D_{tk}$, then $w_k | w_{mk}$ whenever $m \equiv 1 \pmod t$.

Proof: Part (a) is immediate from Corollary 2 with $n = mk$.

Part (b). By (F6), $D_{tk} | D_{ntk}$ for all positive integers n. Then $w_k | D_{ntk}$, whence $w_k | w_{(nt+1)k}$ for all non-negative integers n.

Corollary 4: (a) $w_k | w_{2k}$ if and only if $w_k | r$.

(b) $w_k | w_{3k}$ if and only if $w_k | rS_k$.

(c) $w_k | w_{3k}$ for all $k \geq 1$ if and only if $w_k | r(2s - ar)$ for all $k \geq 1$.

Proof: Part (a) follows from Corollary 3(a) and the corollary to Theorem 1.

Part (b) follows from (F7), Corollary 3(a) and the corollary to Theorem 1.

Part (c): Suppose that $w_k | w_{3k}$ for all $k \geq 1$. By Part (b), $w_k | rS_k$ for all $k \geq 1$. In particular, $w_1 | rS_1$, i.e., $s | ra$. Since $(r,s) = 1$, sa. Let $a = sd$. We shall prove by complete mathematical induction on k that

$$S_k(a,c) = dw_k(r,s;a,c) + c(2 - rd)D_{k-1}(a,c) \quad \text{for all } k \geq 1.$$

1. $$dw_1 + c(2 - rd)D_0 = ds + 0 = a = S_1.$$

2. $$dw_2 + c(2 - rd)D_1 = d(as + cr) + c(2 - rd) = a^2 + 3c = S_2.$$

3. Suppose that the theorem is true for all integers k less than some fixed integer $t \geq 3$.

$$\begin{aligned} S_t &= aS_{t-1} + cS_{t-2} = a[dw_{t-1} + c(2 - rd)D_{t-2}] + c[dw_{t-2} + c(2 - rd)D_{t-3}] \\ &= adw_{t-1} + c(2 - rd)(D_{t-1} - cD_{t-3}) + cdw_{t-2} + c^2(2 - rd)D_{t-3} \\ &= adw_{t-1} + c(2 - rd)D_{t-1} - c^2(2 - rd)D_{t-3} + cdw_{t-2} + c^2(2 - rd)D_{t-3} \\ &= d(aw_{t-1} + cw_{t-2}) + c(2 - rd)D_{t-1} = dw_t + c(2 - rd)D_{t-1}. \end{aligned}$$

Hence if $p | w_n$ and $p | S_n$, then $p | c(2 - rd)D_{n-1}$. So by Theorem 3 and the corollary to Theorem 1, $p | (2 - rd)s$. Thus, by Part (b), if $w_k | w_{3k}$ for all $k \geq 1$, then $w_k | r(2s - ar)$ for all $k \geq 1$.

Conversely, suppose $w_k | r(2s - ar)$ for all $k \geq 1$. Since $w_1 | r(2s - ar)$ and $(r,s) = 1$, $s | a$. Then, letting $a = sd$, it follows from the first half of the proof that $(S_k, w_k) = (2s - ar, w_k)$ for all $k \geq 1$. Hence, by Part (b) and the corollary to Theorem 1, if $w_k | r(2s - ar)$ for all $k \geq 1$, then $w_k | w_{3k}$ for all $k \geq 1$.

Lemma 1: $w_k | w_{2k}$ for all $k \geq 1$ if and only if $w_k w_{k+1} | r$ for all $k \geq 1$.

Proof: The "if" part is immediate by Corollary 4, Part (a).

Suppose that $w_k | w_{2k}$ for all $k \geq 1$. By Corollary 4 (a), $w_k | r$ and $w_{k+1} | r$. But by Theorem 2, $(w_k, w_{k+1}) = 1$. Hence $w_k w_{k+1} | r$.

Lemma 2: If $r \neq 0$ and $(a,r) = 1$, then $w_k | w_{2k}$ for all k only in the following cases:

(a) $r = s = \pm 1$, $a + c = 1$; in which cases $\{w_n\} = \pm\{1, 1, \cdots\}$.

(b) $r = \pm 1$, $s = \mp 1$, $-a + c = 1$; in which cases $\{w_n\} = \pm\{1, -1, 1, -1, \cdots\}$.

(c) $r = \pm 2$, $s = \mp 1$, $a = c = -1$; in which cases $\{w_n\} = \pm\{2, -1, -1, 2, -1, -1, \cdots\}$.

(d) $r = \pm 2$, $s = \pm 1$, $a = 1$, $c = -1$; in which cases $\{w_n\} = \pm\{2, 1, -1, -2, -1, 1, 2, 1, -1, -2, -1, 1, \cdots\}$.

Proof: Suppose $w_n(r,s;a,c)$ is a sequence for which $w_k | w_{2k}$ for all k. Then, by Corollary 4 (a), $w_k | w_{2k}$ for all k. Since $(s,r) = 1$, $s = w_1$ and $w_1 | r$, we may conclude that $s = \pm 1$. Now $w_n(r, 1; a,c) = -w_n(-r, -1; a, c)$ for all n. So it suffices to consider the case where $s = 1$.

Since $w_2 | r$ and $(w_2, r) = (a + cr, r) = (a,r) = 1$, $w_2 = \pm 1$. We shall prove by complete mathematical induction on n that $w_n(r,s;a,c) = (-1)^{n+1} w_n(-r,s;-a,c)$ for all $n \geq 0$:

(1) $w_0(r,s;a,c) = r = (-1)^1(-r) = (-1)^1 w_0(-r,s;-a,c)$.

(2) $w_1(r,s;a,c) = s = (-1)^2(s) = (-1)^2 w_1(-r,s;-a,c)$.

(3) Suppose that the theorem is true for all integers n less than some fixed integer $k \geq 3$.

$$w_k(r,s;a,c) = aw_{k-1}(r,s;a,c) + cw_{k-2}(r,s;a,c) = (-1)^k aw_{k-1}(-r,s;-a,c) + (-1)^{k-1}cw_{k-2}(-r,s;-a,c)$$
$$= (-1)^{k+1}[(-a)w_{k-1}(-r,s;-a,c) + cw_{k-2}(-r,s;-a,c)] = (-1)^{k+1}w_k(-r,s;-a,c).$$

Hence it suffices to consider the case where $w_2 = 1$.

CASE I: Suppose that $a \geq 1$.

Then $c \leq -1$. For were $c \geq 1$, we would have $w_{i+1} > w_i > 1$ for $i \geq 3$, contradicting the fact that $w_i \leq |r|$ for all i. Also since $r = (1-a)/c$, $1 - a \leq c \leq -1$. So $a + c \geq 1$.

(a) If $a + c = 1$, it is easily seen that the sequence reduces to $\{w_0, w_1, \cdots\} = \{1, 1, \cdots\}$.

(b) Suppose that $a + c > 1$. We shall prove by induction on i that $w_i > w_{i-1}$ for $i \geq 3$.

(1) By hypothesis it is true for $i = 3$.

(2) Suppose it to be true for i equal to some fixed integer $n \geq 3$. Then $w_{n+1} = aw_n + cw_{n-1} > w_n(a+c) > w_n$.

But this means that the w_i's form an unbounded sequence, which is impossible since $w_i \leq |r|$ for all i.

CASE II: Suppose that $a \leq -1$.

Since $a + c \,|\, a - 1$, either $c = -1$ or $0 < c < -2a + 1$.

(a) Suppose $c = -1$. Then $w_4 = a^2 - a - 1$ and, since $w_4 | r$, $a^2 - a - 1 \leq 1 - a$. Hence $a^2 \leq 2$, i.e., $a = -1$. Then $r = -2$ and this yields the sequence $\{-2, 1, 1, -2, 1, 1, \cdots\}$.

(b) Suppose $c > 0$. Now $r = (1-a)/c$ and $a + c | r$. So $ac + c^2 | a - 1$.

$$\therefore\ ac + c^2 \leq 1 - a$$
$$\therefore\ a(c+1) \leq 1 - c^2$$
$$\therefore\ a \leq \frac{1-c^2}{c+1} = 1 - c.$$

Also $ac + c^2 \geq a - 1$, whence $a(c-1) \geq -c^2 - 1$. Hence either $c = 1$ or

$$c - 1 \leq -a \leq \frac{c^2+1}{c-1} = (c+1) + \frac{2}{c-1}.$$

Thus case (b) reduces to the following four subcases:

(i) $c = 1$. Now $w_3 | D_3$, i.e., $a + 1 | a^2 + 1$. Since $a^2 + 1 = (a+1)(a-1) + 2$, $a + 1 | 2$. So $a = -2$ or $a = -3$.

1. If $c = 1$ and $a = -2$, then $r = 3$ but $w_5 = -7$.
2. If $c = 1$ and $a = -3$, then $r = 4$ but $w_4 = 7$.

(ii) $a = -c - 1$. Then $w_4 = 2c + 1$, $r = (c+2)/c$ and $w_4 | r$. Hence $2c^2 + c \leq c + 2$. So $c = 1$, a case already considered.

(iii) $a = -c + 1$. But then $a + c = 1$, a case already considered.

(iv) $c = 2$ and $a = -5$. Then $r = 5$ but $w_4 = 17$.

This exhausts all of the possible cases. The other six sequences mentioned in the theorem are precisely those obtained from the sequences $\{1, 1, \cdots\}$ and $\{-2, 1, 1, -2, 1, 1, \cdots\}$ by the permutations of sign outlined at the beginning of the proof.

Theorem 7. If $r \neq 0$, then $w_k | w_{2k}$ for all k only in the cases listed in Lemma 2.

Proof: We shall prove that if $r \neq 0$ and $(a,r) = d > 1$, then w_k fails to divide w_{2k} for some k. The theorem will then follow by Lemma 2. Suppose the contrary, i.e., suppose there exists a sequence $w_n(r,s;a,c)$ such that $w_k | w_{2k}$ for all k. As in Lemma 2, $s = \pm 1$ and, moreover, we need only consider the case where $s = 1$.

Then $w_2 | r$ and $w_2 | D_2$, where $D_2 = a$. So $w_2 | d$. But $d | w_2$, since $w_2 = as + cr$. Thus $w_2 = \pm d$ and, as in the lemma, we need only consider the case where $w_2 = d$.

Suppose $a > 0$ and $d > 0$, $c < 0$ for otherwise the w_i's would become unboundedly large.

Now $d(ad + c) | r$ by Lemma 1 and $r = (d-a)/c \neq 0$. Hence $c(ad + c) | 1 - (a/d)$ and $1 - (a/d) < 0$.

Since $c | 1 - (a/d)$, $1 - (a/d) \leq c < 0$. Since $ad + c | 1 - (a/d)$, $ad + 1 - (a/d) \leq ad + c \leq (a/d) - 1$.

$$\therefore\ ad \leqslant \frac{2a}{d} - 2.$$

$$d^2 \leqslant 2 - \frac{2d}{a} < 2,$$

which is impossible since $d \geqslant 2$. Hence $a < 0$.

Since $cd(ad + c) | a - d,\ a - d \leqslant cd(ad + c) \leqslant d - a$.

Suppose $c < 0$. Now $acd^2 + c^2 d \leqslant d - a$.

$$\therefore\ a(cd^2 + 1) \leqslant d(1 - c^2).$$

$$\therefore\ a \geqslant \frac{d(1 - c^2)}{cd^2 + 1} \geqslant 0,$$

contradicting the fact that $a < 0$. So $a < 0$ and $c > 0$.

Now $acd^2 + c^2 d > a - d$.

$$\therefore\ a(cd^2 - 1) \geqslant -d(c^2 + 1).$$

$$\therefore\ a \geqslant -\frac{d(c^2 + 1)}{cd^2 - 1}.$$

Since $a \leqslant -1$,

$$\frac{c^2 d + d}{cd^2 - 1} \geqslant 1.$$

$$\therefore\ c^2 d + d \geqslant cd^2 - 1.$$

$$\therefore\ d[c(c - d) + 1] \geqslant -1.$$

Since $d > 1$, $d[c(c - d) + 1] \geqslant 0$, whence $c(c - d) \geqslant -1$. Then, since $c \neq 0$ and $(c,d) = 1$, either $c > d$ or $c = 1$ and $d = 2$. But in the latter case, the inequalities

$$-\frac{d(c^2 + 1)}{cd^2 - 1} \leqslant a \leqslant -1$$

imply that $a = -1$, contradicting the fact that $d | a$.

Now, since $cd | a - d,\ c \leqslant 1 - (a/d) < 1 - a$. So $0 < d < c \leqslant 1 - (a/d) < 1 - a$.

Suppose that $a = -d$. Then $a + cr = -a$, i.e., $cr = -2a$ and $a | r$.

CASE I: $r = -a$ and $c = 2$.

Then $ad + c = 2 - a^2$ and $ad + c | -a$. Hence either $a = -1$ or $a = -2$.

But both possibilities are inadmissible since $d = -a > 1$ and $(a,c) = 1$.

CASE II: $r = -2a$ and $c = 1$.

Then $ad + c = 1 - a^2$ and $ad + c | -2a$. But this requires that $1 - a^2$ must divide 2, since $(a, 1 - a^2) = 1$, and this is not satisfied by any integer a. Hence $a \leqslant -2d$.

Suppose that $d > 2$. By Lemma 1, $w_3 w_4 | r$. It follows that $(ad + c)(a^2 d + ac + cd) \geqslant a - d$.

$$\therefore\ a - d \leqslant a^3 d^2 + 2a^2 cd + acd^2 + ac^2 + c^2 d \leqslant a^3 d^2 + 2a^2 cd + acd^2 < d^2 a^3 + 2a^2(1 - a)d + ad^3.$$

$$\therefore\ 0 < d^2 a^3 + 2a^2(1 - a)d + ad^3 - a + d = (d^2 - 2d)a^3 + 2da^2 + (d^3 - 1)a + d < (d^2 - 2d)a^3 + 2da^2$$
$$< a^3 + 2da^2 = a^2(a + 2d) \leqslant 0,$$

a contradiction. Hence $d = 2$. Then

$$ad + c = 2a + c \quad \text{and} \quad r = \frac{2 - a}{c}$$

By Lemma 1, $d(ad + c) | r$. So $4a + 2c > a - 2$.

$$\therefore\ c \geqslant -\frac{3}{2}a - 1 > -a - 1.$$

Hence $-a - 1 < c < -a + 1$, i.e., $c = -a$. But this contradicts the facts that $(a,c) = 1$ and $a < -1$.

Thus we have verified that there is no sequence $w_n(r,s;\,a,c)$ for which $r \neq 0$, $(a,r) > 1$ and $w_k | w_{2k}$ for all k.

CONCLUDING REMARKS

This theorem completes the identification of those sequences for which $w_k | w_{2k}$ for all $k \geqslant 1$; those sequences being

$$\pm \left\{ D_n(a,c) \right\} ; \qquad \pm \left\{ w_n(1,1;a,c) \right\} ,$$

where

$$a + c = 1; \qquad \pm \left\{ w_n(1,-1;a,c) \right\} ,$$

where

$$-a + c = 1; \qquad \pm \left\{ w_n(2,-1;-1,-1) \right\} \quad \text{and} \quad \pm \left\{ w_n(2,1;1,-1) \right\} .$$

These sequences, it is clear are precisely those for which $w_k | w_{mk}$ for all integers $k \geqslant 1$ and $m \geqslant 0$. In fact, an inspection of the proofs of Lemma 2 and Theorem 7 discloses that these are the only sequences for which $w_k | w_{2k}$ for $1 \leqslant k \leqslant 5$ and $\left\{ |w_k| \,\middle|\, k - 1, 2, \cdots \right\}$ is bounded.

REFERENCES

1. R. D. Carmichael, "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$," *Annals of Mathematics,* 2, 15 (1913), pp. 30–70.
2. H. Siebeck, "Die recurrenten Reihen, vom Standpuncte der Zahlentheorie aus betrachtet," *Journal für die reine und angewandte Mathematik,* XXXIII, 1(1846), pp. 71–77.
3. D. Zeitlin, "Power Identities for Sequences Defined by $W_{n+2} = dW_{n+1} - cW_n$," *The Fibonacci Quarterly,* Vol. 3, No. 4 (Dec. 1965), pp. 241–256.

****