ON r^{th}-ORDER RECURRENCES*

LAWRENCE SOMER
George Washington University, Washington, D.C. 20052

(Submitted August 1985)

This note will generalize results obtained by Wyler [5] concerning periods of second-order recurrences.

Let $r \geqslant 2$ and let (u) be an r^{th}-order linear recurrence over the rational integers satisfying the recursion relation

$$u_{n+r} = a_1 u_{n+r-1} - a_2 u_{n+r-2} + \cdots + (-1)^{r+1} a_r u_n \tag{1}$$

with initial terms $u_0 = u_1 = \cdots = u_{r-2} = 0$, $u_{r-1} = 1$. Then (u) is called a unit sequence with coefficients $a_1, a_2, \ldots, a_r$. For a positive integer M, the primitive period of (u) modulo M, denoted by $K(M)$, is the least positive integer m such that $u_{n+m} \equiv u_n \pmod{M}$ for all nonnegative integers n greater than or equal to some fixed integer n_0. It is known that the primitive period modulo M of a unit sequence (u) is a period modulo M of any other recurrence satisfying the same recursion relation (see [4], pp. 603-04). The rank of (u) modulo M, denoted by $k(M)$, is the least integer m such that $u_{n+m} \equiv su_n \pmod{M}$ for some residue s and for all integers n greater than or equal to some fixed nonnegative integer n_0. We call s the principal multiplier of (u) modulo M. If $(a_r, M) = 1$, then it is known from [1] that (u) is purely periodic modulo M and $K(M) | k(M)$. Furthermore, if $(a_r, M) = 1$, Carmichael [1] has shown that the principal multiplier s is a unit modulo M and $K(M)/k(M) = E(M)$ is the exponent of the multiplier s modulo M. In this paper, we will put constraints on $K(M)$ given $k(M)$ and the exponent of a_r modulo M.

Our two main results are Theorems 1 and 2. Theorem 2 is a refinement of Theorem 1.

Theorem 1: Let (u) be a unit sequence with coefficients $a_1, a_2, \ldots, a_r$. Let $M \geqslant 2$ be a positive integer such that $(a_r, M) = 1$. Let h be the exponent of a_r modulo M. Let $k = k(M)$ and $K = K(M)$. Let H be the least common multiple of h and k. Then $H | K$ and $K | rH$.

Theorem 2: Let (u) be a unit sequence with coefficients $a_1, a_2, \ldots, a_r$. Let $M \geqslant 2$ be a positive integer such that $(a_r, M) = 1$. Let h, k, K, and H be defined as in Theorem 1. Let

$$r = \prod_{i=1}^{n} p_i^{\alpha_i},$$

where the p_i are distinct primes and $a_i \geqslant 1$. Let

$$h = \left(\prod_{i=1}^{n} p_i^{\beta_i}\right) h', \quad k = \left(\prod_{i=1}^{n} p_i^{\gamma_i}\right) k',$$

This note is based partly on results in the author's Ph.D. Dissertation, The University of Illinois at Urbana-Champaign, 1985.

where $\beta_i \geqslant 0$, $\gamma_i \geqslant 0$, and $(h', r) = (k', r) = 1$. Let j vary over all the indices i, $1 \leqslant i \leqslant n$, such that $\beta_i > \gamma_i$. Let $c = 1$ if there is no subscript i such that $\beta_i > \gamma_i$. Otherwise, let

$$c = \prod_j p_j^{\alpha_j}.$$

Then

$$cH \mid K$$

and

$$K \mid k(rH/k,\ \phi(M)),$$

where $\phi(M)$ denotes Euler's totient function.

To prove Theorems 1 and 2, we will need the following lemmas.

Lemma 1: For the unit sequence (u) given in (1), define the persymmetric determinant

$$D_n^{(r)}(u) = \begin{vmatrix} u_n & u_{n+1} & \cdots & u_{n+r-1} \\ u_{n+1} & u_{n+2} & \cdots & u_{n+r} \\ \cdots & \cdots & \cdots & \cdots \\ u_{n+r-1} & u_{n+r} & & u_{n+2r-2} \end{vmatrix}$$

Then

$$D_{n+1}^{(r)}(u) = a_r D_n^{(r)}(u).$$

Proof: This is Heymann's Theorem and a proof is given in [2, ch. 12.12]. ∎

Lemma 2: Let $k = k(M)$. Suppose

$$u_m \equiv u_{m+1} \equiv \cdots \equiv u_{m+r-2} \equiv 0 \pmod{M}$$

and $(a_r, M) = 1$. Then $k \mid m$. Furthermore,

$$u_{mi+n} \equiv u_{m+r-1}^i u_n \pmod{M} \tag{2}$$

and for all non-negative integers n,

$$u_{m+r-1}^r \equiv a_r^m \pmod{M}. \tag{3}$$

In particular, if s is the principal multiplier of (u), then

$$s^r \equiv a_r^k \pmod{M}.$$

Proof: Suppose $m = tk + d$, where $0 \leqslant d < k$. Since (u) is purely periodic modulo M, it follows that, for $0 \leqslant n \leqslant r - 2$,

$$0 \equiv u_{m+n} \equiv su_{m+n-k} \equiv s^2 u_{m+n-2k} \equiv \cdots \equiv s^t u_{m+n-tk} = s^t u_{d+n} \pmod{M},$$

where s is the principal multiplier of (u) modulo M. However, if $d > 0$, this is impossible since s is a unit modulo M and, by definition, k is the smallest positive integer j such that $u_{j+n} \equiv 0 \pmod{M}$ for $0 \leqslant n \leqslant r - 2$. Thus, $d = 0$ and $k \mid m$.

We now note that

$$u_{m+n} \equiv u_{m+r-1} u_n \pmod{M} \tag{4}$$

for $0 \leqslant n \leqslant r - 1$. It follows from the linearity of the r^{th}-order recursion relation defining (u) that (4) holds for all nonnegative integers n, and u_{m+r-1}

is a multiplier modulo M, though not necessarily principal, of (u). By applying congruence (4) repeatedly, we obtain

$$\begin{aligned} u_{mi+n} &= u_{m+(m(i-1)+n)} \equiv u_{m+r-1}u_{m(i-1)+n} = u_{m+r-1}u_{m+(m(i-2)+n)} \\ &\equiv u^2_{m+r-1}u_{m(i-2)+n} \equiv \cdots \equiv u^i_{m+r-1}u_n \pmod{M}, \end{aligned}$$

and congruence (2) holds.

To prove (3), we note that since $u_m \equiv u_{m+1} \equiv \cdots \equiv u_{m+r-2} \equiv 0 \pmod{M}$, one easily calculates that

$$D_m^{(r)}(u) \equiv (-1)^{r(r-1)/2}u^r_{m+r-1} \pmod{M}.$$

Moreover, since $u_0 = u_1 = \cdots = u_{r-2} = 0$ and $u_{r-1} = 1$,

$$D_0^{(r)}(u) = (-1)^{r(r-1)/2}.$$

By applying Lemma 1 m times, we now obtain

$$D_m^{(r)}(u) \equiv (-1)^{r(r-1)/2}u^r_{m+r-1} \equiv a^m D_0^{(r)}(u) = a^m_r(-1)^{r(r-1)/2} \pmod{M},$$

and congruence (3) is seen to hold. Finally, noting that $s \equiv u_{k+r-1} \pmod{M}$, the lemma now follows. ∎

We are now ready for the proofs of Theorems 1 and 2.

Proof of Theorem 1: Note that $u_{K+r-1} \equiv u_{r-1} = 1 \pmod{M}$. By Lemma 2,

$$u^r_{K+r-1} \equiv a^K_r \equiv 1 \pmod{M}.$$

Thus, K is a multiple of h. Since $k|K$, K is also a multiple of H. On the other hand, by Lemma 2,

$$u_{rH} \equiv u_{rH+1} \equiv \cdots \equiv u_{rH+r-2} \equiv 0 \pmod{M}$$

and

$$u_{rH+r-1} \equiv u^r_{H+r-1} \equiv a^H_r \equiv 1 \pmod{M}.$$

Hence, rH is a multiple of K and we are done. ∎

Proof of Theorem 2: By Theorem 1, $K|rH$. Since $K = kE(M)$ and $E(M)|\phi(M)$, it follows that

$$K|k(rH/k,\ \phi(M)).$$

For a given index j, let $\delta_j = \alpha_j + \beta_j$. Then it follows from the definitions of c and H that

$$p_j^{\delta_j} \,\|\, cH \quad \text{and} \quad p_j^{\delta_j} \,\|\, rH,$$

where $p_j^x \,\|\, N$ means x is the highest power of p_j dividing N. Since $H|K$ by Theorem 1 and $cH|rH$, it suffices to prove that if p_j is a prime dividing c, then

$$K \nmid (rH/p_j).$$

By Lemma 2, we thus need to show that

$$u_{(rH/p_j)+r-1} \not\equiv 1 \pmod{M}.$$

Note that $p_jk|H$ since $\beta_j > \gamma_j$. Thus, $rH/p_j = kN$ for some integer N. Moreover, $r|N$ since $k|H/p_j$. By Lemma 2,

$$\begin{aligned} u_{(rH/p_j)+r-1} &= u_{kN+r-1} \equiv u^N_{k+r-1}u_{r-1} = (u^r_{k+r-1})^{N/r} \\ &\equiv (s^r)^{N/r} \equiv (a^k_r)^{N/r} = a_r^{H/p_j} \pmod{M}. \end{aligned}$$

Now,

$$p_j^{\beta_j-1} \,\|\, (H/p_j),\ p_j^{\beta_j} \,\|\, h.$$

Thus,

$$u_{(rH/p_j)+r-1} \equiv a_r^{H/p_j} \not\equiv 1 \pmod{M}.$$

Consequently, $K \nmid (rH/p_j)$ and we are done. ■

REFERENCES

1. R. D. Carmichael. "On Sequences of Integers Defined by Recurrence Relations." *Quart. J. Pure Appl. Math.* 48 (1920):343-72.
2. L. M. Milne-Thomson. *The Calculus of Finite Differences*. London: Macmillan, 1960.
3. L. Somer. "The Divisibility and Modular Properties of k^{th}-Order Linear Recurrences Over the Ring of Integers of an Algebraic Number Field with Respect to Prime Ideals." Ph.D. dissertation, The University of Illinois at Urbana-Champaign, 1985.
4. M. Ward. "The Arithmetical Theory of Linear Recurring Series." *Trans. Amer. Math. Soc.* 35 (1933):600-28.
5. O. Wyler. "On Second-Order Recurrences." *Amer. Math. Monthly* 72 (1965): 500-06.

◆◇◆◇◆