

SOME OBSERVATIONS CONCERNING A STATEMENT OF MARSHALL HALL, JR.

E. L. Roettger
Department of General Education, Mount Royal University, Calgary, Alberta, Canada
eroettger@mtroyal.ca

H. C. Williams
Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada
hwilliam@ucalgary.ca

Received: 5/27/26, Accepted: 10/14/26, Published: 11/23/26

Abstract

This paper attempts to determine what might have been known by Morgan Ward about the problem of determining certain nondegenerate third-order linear recurrences with initial terms 0, 1 that are also divisibility sequences. It was mentioned by Marshall Hall, Jr. that Ward had completely characterized these; however, it appears that this might not be the case, as nowhere in Ward's published works is such work mentioned. In this investigation we attempt to reconstruct Ward's reasoning concerning this problem.

1. Introduction

For given integers P_1, P_2, P_3, T_0, T_1, and T_2, let (T_n) be a sequence of integers satisfying the third-order linear recurrence

$$T_{n+3} = P_1 T_{n+2} - P_2 T_{n+1} + P_3 T_n, \tag{1}$$

where $P_3 \neq 0$. We say that a sequence of integers (S_n) is a *divisibility sequence* (DS) if $S_n \mid S_m$ whenever $n \mid m$ for all $0 < n < m$. Note in particular that if $S_n = 0$, then $S_m = 0$ for all multiples m of n.

Prior to completing his PhD dissertation entitled, *An Isomorphism Between Linear Recurring Sequences and Algebraic Rings* [7], a work that was greatly influenced

DOI: 10.5281/zenodo.24473303

by two papers of Morgan Ward [12, 13], Marshall Hall Jr. conducted some research on (T_n). In [6, Theorem II] he showed that if (T_n) is a divisibility sequence and $T_0 \neq 0$, then the only possible divisors of T_n must divide $\gcd(T_0, P_3)$, but if $T_0 = 0$, and p is any prime such that $p \nmid P_3$, then $p \mid T_n$ for some $n \geq 1$. Because of this Hall confined his attention in [6] to divisibility sequences in (T_n), where $T_0 = 0$.

Let

$$f(x) = x^3 - P_1 x^2 + P_2 x - P_3$$

be the *characteristic polynomial* of (T_n). The main result of [6] is that if $f(x)$ is irreducible over the rationals $\mathbb{Q}$, $\gcd(P_2, P_3) = 1$, and $T_0 = 0$, then the sequence (T_n) cannot be a DS. Several years later, Ward [19] eliminated the need for $\gcd(P_2, P_3) = 1$ in this result.

In Section 4 of [6] Hall remarked that if the sequence $(T_n) = (u_n^2)$, where u_n is a certain Lucas or Lehmer sequence (see Section 4 below), then T_n satisfies (1) and T_n is a DS. (This is also true for $T_n = (u_n)$, where u_n is a certain Lucas sequence.) He also included a footnote concerning this:

> Since completing this paper I have learned from Dr. Morgan Ward that he has been able to show that [these are] the only type if $f(x)$, the characteristic polynomial, has a linear and an irreducible quadratic factor...

Unfortunately, nowhere in any of Ward's published work does any mention of this investigation appear. This seems most curious because it would have been appropriate to provide some remarks concerning it in [17] or especially in [19, pp. 87–88]. Thus, in spite of Hall's authority, we would consider this still to be an open problem, except that very recently the more general problem of determining all the nondegenerate (see below) third-order linear recurrence sequences (T_n) with $T_0 = 0$ and $T_1 = 1$, which are also divisibility sequences, has been completely solved by Andrew Granville [5, Section 11.5]. In doing this, Granville made use of some very deep results, such as an application of the Schmidt/Schlickewei subspace theorem from the theory of Diophantine approximation, due to Corvaja and Zannier. None of these results would have been available to Ward in 1936.

Thus, the question that remains is why Ward thought he had proved the result mentioned in Hall's footnote. Of course, it is possible Hall misinterpreted Ward's remark, but that seems unlikely, as both correspondents were very aware of the issues involved. It seems more plausible that Ward made a mistake which he later realized. The purpose of this paper is to investigate this question by making use of techniques that Ward might have employed. While much of the material which follows was known to Ward (see especially [13, 16, 17]), we have included it here to keep this paper mostly self-contained.

2. Some Preliminary Remarks

We first observe, as did Hall, that if (T_n) above is a divisibility sequence with $T_0 = 0$, we may assume with no loss of generality that $T_1 = 1$. Let α, β, and γ be the roots of $f(x) = 0$ and put

$$\Delta = [(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)]^2 = P_1^2P_2^2 + 18P_1P_2P_3 - 4P_2^3 - 4P_1^3P_3 - 27P_3^2.$$

We will assume in what follows that $\Delta \neq 0$. This is certainly the case if $f(x)$ has an irreducible quadratic factor. Since (T_n) satisfies (1), there must exist constants c_1, c_2, and c_3, independent of n, such that

$$T_n = c_1\alpha^n + c_2\beta^n + c_3\gamma^n. \tag{2}$$

Furthermore, if T_n is given by (2), then (T_n) must also satisfy (1).

We will say that (T_n) is *degenerate* if the ratio of two roots of $f(x)$ is a root of unity. Otherwise, we say that (T_n) is *nondegenerate*. We say the term T_k is a *zero* of the recurrence (T_n) if $T_k = 0$. In 1935 Mahler [9] showed that if (T_n) is nondegenerate, then $|T_n|$ will tend to infinity as n does; thus, the number of zeros of a nondegenerate (T_n) must be finite. Indeed, we now know (see Beukers [3]) that such a sequence can have at most six zeros. We see, then, that if (T_n) is a nondegenerate DS, then T_k can be 0 only when $k = 0$.

A positive integer which divides every term of (T_n) beyond a certain point is called a *null divisor* of (T_n). If (T_n) has no null divisors except for 1, Ward called (T_n) *primary* (see [17]).

Lemma 1. *The sequence (T_n) is primary if and only if* $\gcd(P_1T_2, P_2, P_3) = 1$.

Proof. If p is a prime and $p \mid \gcd(P_1T_2, P_2, P_3)$, then from (1),

$$T_3 = P_1T_2 - P_2T_1 + P_3T_0;$$

hence, $p \mid T_3$. By induction on parameter n in (1) we have $p \mid T_n$ for all $n \geq 3$. Thus, p is a null divisor of (T_n), and therefore (T_n) is not primary.

Next, suppose p is a prime null divisor of (T_n) and that p divides T_n for all $n \geq k$, where $k \geq 0$ is minimal. Since $T_0 = 0$ and $T_1 = 1$, we cannot have $k = 0$ or 1. If $k = 2$, then since $p \mid T_n$ $(n \geq 2)$ and (from (1))

$$T_4 = P_1T_3 - P_2T_2 + P_3T_1,$$

we have $p \mid P_3$. Also, from (1),

$$T_3 = P_1T_2 - P_2T_1 + P_3T_0 = P_1T_2 - P_2T_1$$

and $p \mid P_2$. Thus $p \mid \gcd(P_1T_2, P_2, P_3)$. Now suppose $k \geq 3$. Here, $p \mid T_k$, $p \mid T_{k+1}$, and $p \mid T_{k+2}$; however, $p \nmid T_{k-1}$. Since

$$T_{k+2} = P_1T_{k+1} - P_2T_k + P_3T_{k-1},$$

we have $p \mid P_3$. Similarly, since

$$T_{k+1} = P_1 T_k - P_2 T_{k-1} + P_3 T_{k-2},$$

we also have $p \mid P_2$. Finally, notice that if $p \mid \gcd(P_2, P_3)$, then

$$T_{m+3} \equiv P_1 T_{m+2} \pmod{p}.$$

By induction on m we have

$$T_m \equiv P_1^{m-2} T_2 \pmod{p}$$

for $m \geq 3$. Since $p \mid T_k$ for some $k \geq 3$, we have $p \mid P_1 T_2$, and therefore

$$p \mid \gcd(P_1 T_2, P_2, P_3).$$

□

From this it is easy to show the following.

Lemma 2. *If (T_n) is primary, then for all $n > 0$ we have $p \nmid T_n$ when $p \mid \gcd(P_2, P_3)$.*

Proof. Let p be any prime divisor of P_2 and P_3. We have

$$T_{n+3} \equiv P_1 T_{n+2} \pmod{p}$$

when $n \geq 0$. By induction, $T_m \equiv P_1^{m-2} T_2$, hence $p \nmid T_m$ $(m \geq 3)$ because $p \nmid T_2 P_1$ by Lemma 1. Thus, $p \mid T_0$ ($T_0 = 0$ and $T_1 = 1$), but $p \nmid T_n$ for $n > 0$. □

We next examine the question of when (T_n) can be a divisibility sequence.

3. A Criterion for (T_n) To Be a Divisibility Sequence

We begin this section with a simple criterion for (T_n) to be a DS.

Proposition 1. *The sequence (T_n) is a DS if and only if $T_n \mid T_{2n}$ for all $n \geq 1$.*

Proof. If (T_n) is a divisibility sequence, then $T_n \mid T_{2n}$ for all $n \geq 1$. Suppose that $T_n \mid T_{2n}$ for all $n \geq 1$. For any fixed $n \geq 1$, put $P_1(n) = \alpha^n + \beta^n + \gamma^n$ and $P_2(n) = \alpha^n \beta^n + \beta^n \gamma^n + \gamma^n \alpha^n$. Clearly, $P_1(n)$, $P_2(n), P_3^n \in \mathbb{Z}$ and α^n, β^n, and γ^n are the roots of

$$x^3 - P_1(n)x^2 + P_2(n)x - P_3^n = 0.$$

It follows that since $T_{kn} = c_1 \alpha^{kn} + c_2 \beta^{kn} + c_3 \gamma^{kn}$, we have

$$T_{(k+3)n} = P_1(n) T_{(k+2)n} - P_2(n) T_{(k+1)n} + P_3^n T_{kn}.$$

Since $T_n \mid T_0$, $T_n \mid T_n$, and $T_n \mid T_{2n}$, we easily see by induction that $T_n \mid T_{mn}$ for any $m \geq 0$. Since this holds for all $n \geq 1$, we see that (T_n) is a divisibility sequence. □

From (2) we note that

$$c_1 + c_2 + c_3 = T_0 = 0,$$
$$c_1\alpha + c_2\beta + c_3\gamma = T_1 = 1,$$

and

$$c_1\alpha^2 + c_2\beta^2 + c_3\gamma^2 = T_2.$$

We also know that there exist three sequences of integers (X_n), (Y_n), (Z_n) such that

$$\alpha^n = X_n + \alpha Y_n + \alpha^2 Z_n, \tag{3}$$
$$\beta^n = X_n + \beta Y_n + \beta^2 Z_n, \tag{4}$$

and

$$\gamma^n = X_n + \gamma Y_n + \gamma^2 Z_n. \tag{5}$$

Hence,

$$T_n = (c_1 + c_2 + c_3)X_n + (c_1\alpha + c_2\beta + c_3\gamma)Y_n + (c_1\alpha^2 + c_2\beta^2 + c_3\gamma^2)Z_n,$$

which means that

$$T_n = Y_n + T_2 Z_n. \tag{6}$$

Also,

$$\alpha^3 = P_1\alpha^2 - P_2\alpha + P_3$$

and

$$\alpha^4 = P_1\alpha^3 - P_2\alpha^2 + P_3\alpha = (P_1^2 - P_2)\alpha^2 + (P_3 - P_1P_2)\alpha + P_1P_3.$$

We have the initial conditions:

$$\begin{aligned} &X_0 = 1, \quad Y_0 = 0, \quad Z_0 = 0,\\ &X_1 = 0, \quad Y_1 = 1, \quad Z_1 = 0,\\ &X_2 = 0, \quad Y_2 = 0, \quad \text{and} \quad Z_2 = 1. \end{aligned}$$

Furthermore, by solving Equations (3), (4), and (5) for X_n, Y_n, and Z_n, we see that (X_n), (Y_n), and (Z_n) satisfy the recurrence (1).

These sequences (X_n), (Y_n), and (Z_n), first mentioned by Bell [2], Ward's PhD advisor, are now called the *impulse sequences* with respect to $f(x)$ (see Everest et al. [4, Section 1.1.4]). Ward was certainly aware of these sequences because he made use of them in [14]. Notice that since

$$P_3^n = \alpha^n\beta^n\gamma^n = (X_n + \alpha Y_n + \alpha^2 Z_n)(X_n + \beta Y_n + \beta^2 Z_n)(X_n + \gamma Y_n + \gamma^2 Z_n)$$

we have

$$P_3^n = X_n^3 + P_3Y_n^3 + P_3^2Z_n^3 + (P_1P_2 - 3P_3)X_nY_nZ_n + P_1X_n^2Y_n + P_2X_nY_n^2 + (P_1^2 - 2P_2)X_n^2Z_n + (P_2^2 - 2P_1P_3)X_nZ_n^2 + P_1P_3Y_n^2Z_n + P_2P_3Y_nZ_n^2. \tag{7}$$

Also,

$$\begin{aligned}\alpha^{n+m} &= X_{n+m} + Y_{n+m}\alpha + Z_{n+m}\alpha^2 \\ &= (X_n + Y_n\alpha + Z_n\alpha^2)(X_m + Y_m\alpha + Z_m\alpha^2) \\ &= X_nX_m + P_3(Z_nY_m + Y_nZ_m) + P_1P_3Z_nZ_m \\ &\quad + \alpha((X_nY_m + Y_nX_m) - P_2(Z_nY_m + Y_nZ_m) + (P_3 - P_1P_2)Z_nZ_m) \\ &\quad + \alpha^2((Z_nX_m + Y_nY_m + X_nZ_m) + P_1(Z_nY_m + Y_nZ_m) + (P_1^2 - P_2)Z_nZ_m).\end{aligned}$$

There are similar formulas involving β and γ. Since $\Delta \neq 0$, we can solve for X_{n+m}, Y_{n+m}, Z_{n+m} as follows:

$$\begin{aligned}X_{n+m} &= X_nX_m + P_3(Z_nY_m + Y_nZ_m) + P_1P_3Z_nZ_m, \\ Y_{n+m} &= X_nY_m + Y_nX_m - P_2(Z_nY_m + Y_nZ_m) + (P_3 - P_1P_2)Z_nZ_m,\end{aligned}$$

and

$$Z_{n+m} = Z_nX_m + Y_nY_m + X_nZ_m + P_1(Z_nY_m + Y_nZ_m) + (P_1^2 - P_2)Z_nZ_m.$$

These are the addition formulas for (X_n), (Y_n), and (Z_n). Since, by (6),

$$T_{n+m} = Y_{n+m} + T_2Z_{n+m},$$

we get

$$T_{n+m} = X_nT_m + X_mT_n + T_2Y_nY_m + (T_2P_1 - P_2)(Z_nY_m + Y_nZ_m) + (T_2(P_1^2 - P_2) + (P_3 - P_1P_2))Z_nZ_m. \tag{8}$$

Putting $n = m$, we get the doubling formulas:

$$X_{2n} = X_n^2 + P_1P_3Z_n^2 + 2P_3Y_nZ_n, \tag{9}$$

$$Y_{2n} = (P_3 - P_1P_2)Z_n^2 + 2X_nY_n - 2P_2Y_nZ_n, \tag{10}$$

and

$$Z_{2n} = Y_n^2 + (P_1^2 - P_2)Z_n^2 + 2P_1Y_nZ_n + 2X_nZ_n. \tag{11}$$

Thus, by (6), (10), and (11), we have

$$\begin{aligned}T_{2n} &= Y_{2n} + T_2Z_{2n} \\ &= (P_3 - P_1P_2)Z_n^2 + 2X_nY_n - 2P_2Y_nZ_n \\ &\qquad + T_2(Y_n^2 + (P_1^2 - P_2)Z_n^2 + 2P_1Y_nZ_n + 2X_nZ_n) \\ &= (P_3 - P_1P_2 + (P_1^2 - P_2)T_2)Z_n^2 + 2X_n(Y_n + T_2Z_n) + 2(P_1T_2 - P_2)Y_nZ_n \\ &\qquad + T_2Y_n^2.\end{aligned}$$

Since (T_n) must be a divisibility sequence, we have $T_n \mid T_{2n}$, which holds if and only if

$$T_n \mid (P_3 - P_1P_2)Z_n^2 + (P_1^2 - P_2)T_2Z_n^2 + 2P_1T_2Y_nZ_n - 2P_2Y_nZ_n + T_2Y_n^2. \quad (12)$$

Also, since $Y_n \equiv -T_2Z_n \pmod{T_n}$, we find that (12) holds if and only if

$$T_n \mid (P_3 - P_1P_2)Z_n^2 + (P_1^2 - P_2)T_2Z_n^2 - 2P_1T_2^2Z_n^2 + 2P_2T_2Z_n^2 + T_2^3Z_n^2$$

if and only if

$$T_n \mid Z_n^2(T_2^3 - 2P_1T_2^2 + (P_1^2 + P_2)T_2 + P_3 - P_1P_2).$$

Consider the polynomial

$$h(x) = x^3 - 2P_1x^2 + (P_1^2 + P_2)x + P_3 - P_1P_2 = -f(P_1 - x).$$

We have proved that if (T_n) is a divisibility sequence, we must have $T_n \mid h(T_2)Z_n^2$ for all $n \geq 1$. We next show that if $T_n \mid h(T_2)Z_n^2$ for all $n \geq 1$, then (T_n) must be a divisibility sequence. Since we must have $T_n \mid T_{2n}$ for all $n \geq 1$, we see that (T_n) is a DS by Proposition 1.

We have proved the following result.

Theorem 1. *The sequence (T_n) is a divisibility sequence if and only if*

$$T_n \mid h(T_2)Z_n^2 \quad \textit{for all } n > 0.$$

Unfortunately, Theorem 1 is by itself not sufficient to identify the exact sequences (T_n) that are divisibility sequences, but it can be used to discover certain properties of such sequences. In order to proceed, we first need to summarize some basic properties of the Lucas and Lehmer sequences.

4. The Lucas and Lehmer Sequences

Let P, Q be integers and let ψ, χ be the zeros of $x^2 - Px + Q$. We define the Lucas sequences (v_n) and (u_n) by

$$v_n = v_n(P, Q) = \psi^n + \chi^n \quad \text{and} \quad u_n = u_n(P, Q) = \frac{\psi^n - \chi^n}{\psi - \chi}.$$

Put $D = (\psi - \chi)^2 = P^2 - 4Q$. We call D, the discriminant of the characteristic polynomial $x^2 - Px + Q$, the *discriminant* of (v_n) or (u_n). These sequences have been the objects of much study, and some of their basic properties can be found in,

for example, [1, Chapter 2], [20, Chapter 4] or in Ribenboim [10, Chapter 2, IV]. Both of these sequences satisfy the second-order linear recurrence

$$x_{n+2} = Px_{n+1} - Qx_n. \tag{13}$$

Notice that by (13) we have

$$u_n \equiv P^{n-1} \pmod{Q} \quad (n \geq 1). \tag{14}$$

We will require the following identities which are mentioned in either of the above-cited works:

$$v_n^2 - Du_n^2 = 4Q^n, \tag{15}$$
$$v_{2n} = v_n^2 - 2Q^n, \tag{16}$$
$$2v_{n+m} = v_n v_m + Du_n u_m, \tag{17}$$
$$2u_{n+m} = v_n u_m + v_m u_n, \tag{18}$$
$$v_{n+m} = v_n v_m - Q^m v_{n-m}, \tag{19}$$

and

$$u_n^2 - u_{n-1}u_{n+1} = Q^{n-1}. \tag{20}$$

We also have the following results.

Theorem 2. *If p is any odd prime such that $p \nmid Q$ and $\varepsilon = (D|p)$, then*

$$u_p \equiv \varepsilon \pmod{p} \quad \textit{and} \quad v_p \equiv P \pmod{p}.$$

From this theorem, it is not difficult to deduce that if $\varepsilon \neq 0$, then

$$v_{p^2-1} \equiv 2 \pmod{p} \quad \text{and} \quad u_{p-\varepsilon} \equiv 0 \pmod{p}; \quad \text{also,} \quad u_{p^2-1} \equiv 0 \pmod{p};$$

hence, by (17) and (18), we get

$$v_{p^2-1+n} \equiv v_n \pmod{p} \quad \text{and} \quad u_{p^2-1+n} \equiv u_n \pmod{p} \tag{21}$$

and if $\varepsilon = 0$, then

$$v_{2p(p-1)} \equiv 2 \pmod{p} \quad \text{and} \quad u_{2p(p-1)} \equiv 0 \pmod{p}.$$

Theorem 3. *If p is any odd prime such that $p \nmid Q$ and $p \mid u_n$, then $\rho \mid n$, where ρ is the least positive integer such that $p \mid u_\rho$.*

In [8] Lehmer extended the Lucas sequences (see also [1, Section 4.4]) by replacing P by $\sqrt{R}$, where R is an integer. In this case we have $D = R - 4Q$, which means that D can be 2 or 3 (mod 4), something that is impossible for the Lucas sequences.

Of course, if R is not a perfect square, then we see that $u_n(\sqrt{R}, Q)$ and $v_n(\sqrt{R}, Q)$ are not always going to be integers for $n \geq 1$. However, if we define

$$\bar{u}_n(R,Q) = u_n(\sqrt{R},Q) \quad \text{and} \quad \bar{v}_n(R,Q) = v_n(\sqrt{R},Q)/\sqrt{R} \quad (2 \nmid n)$$

and

$$\bar{u}_n(R,Q) = u_n(\sqrt{R},Q)/\sqrt{R} \quad \text{and} \quad \bar{v}_n(R,Q) = v_n(\sqrt{R},Q) \quad (2 \mid n),$$

then it is easy to see that both $(\bar{u}_n)$ and $(\bar{v}_n)$ satisfy the fourth-order recurrence

$$x_{n+4} = (R - 2Q)x_{n+2} - Q^2 x_n.$$

Since $\bar{u}_0(R,Q) = 0$, $\bar{u}_1(R,Q) = \bar{u}_2(R,Q) = 1$, $\bar{u}_3(R,Q) = R - Q$, $\bar{v}_0(R,Q) = 2$, $\bar{v}_1(R,Q) = 1$, $\bar{v}_2(R,Q) = R - 2Q$, and $\bar{v}_3(R,Q) = R - 3Q$, we see by induction that $\bar{u}_n$ and $\bar{v}_n$ will always be integers whenever $n \geq 0$. We call the sequences $(\bar{u}_n) = (\bar{u}_n(R,Q))$ and $(\bar{v}_n) = (\bar{v}_n(R,Q))$ the *Lehmer sequences*. Since the identity relations given above hold for non-integral values of P and Q, it is possible to derive several properties of these sequences which are analogous to corresponding results concerning the Lucas sequences. It is well known that both (u_n) and $(\bar{u}_n)$ are divisibility sequences.

5. The Rank of Appearance of p in (A_n)

In what follows we will let (A_n) denote any nondegenerate and primary (T_n) which is also a DS and p denote any prime which is not a null divisor of (A_n). We next prove some results concerning (A_n) modulo a prime p.

Definition 1. Let ω_1 be the least positive integer (if it exists) such that $p \mid A_{\omega_1}$. We define the increasing sequence $\omega_1, \omega_2, \ldots, \omega_j \in \mathbb{Z}$ by $p \mid A_{\omega_i}$ and $\omega_i \nmid \omega_j$ $(1 \leq i < j)$. We call each ω_i in this sequence a *rank of appearance* of p.

Definition 2. If $p \mid A_n$ implies that $\omega_1 \mid n$, then p has a single rank of appearance in (A_n). Such a sequence is said to be *monoapparitic* modulo p and the prime p is said to be *monoapparitic* in (A_n). In this case we denote ω_1 by $\omega(p)$ or ω.

It is of some interest to determine when $\omega(p)$ must exist.

Theorem 4. *If p is a prime such that $p \nmid P_3$, then $\omega(p)$ must exist for (A_n).*

Proof. Let $\mathbf{V}_n$ denote the row vector (A_n, A_{n+1}, A_{n+2}). By (1) we have

$$\mathbf{V}_{n+1} = \mathbf{V}_n C,$$

where C is the 3×3 companion matrix for $f(x)$. Note that the determinant of C is P_3, and since $p \nmid P_3$, C is invertible modulo p. By induction, we have

$$\mathbf{V}_n = \mathbf{V}_0 C^n.$$

Since there are only a finite number of distinct residues modulo p, there can only be a finite number of matrices C^k modulo p. Thus, by the Dirichlet pigeonhole principle, there must exist integers r (≥ 0), and s (≥ 1) such that

$$C^{r+s} \equiv C^r \pmod{p}.$$

Since C is invertible modulo p, we get $C^s \equiv I \pmod{p}$, where I is the 3×3 identity matrix. Thus,

$$\mathbf{V}_s \equiv \mathbf{V}_0 C^s \equiv \mathbf{V}_0 \pmod{p}$$

and therefore

$$A_s \equiv 0 \pmod{p}$$

with $s \geq 1$. It follows that $\omega(p)$ must exist. □

In [18] Ward proved that primes have only finitely many ranks of appearance in a general linear divisibility sequence (LDS). In this paper we shall be concerned with the special case of an LDS of order 3. We are now able to deduce Theorem 5.

Theorem 5. *If (A_n) is an LDS of order 3 and $p \nmid h(A_2)P_3$, then p is monoapparatic in (A_n).*

Proof. Let ω be the least rank of appearance of p in (A_n) and suppose $p \mid A_\kappa$. Put

$$\kappa = \omega q + r \quad (0 \leq r < \omega).$$

By Theorem 1, we must have $A_{q\omega} \mid h(A_2)Z_{q\omega}^2$. Also, since $p \mid A_{q\omega}$, we have $p \mid Z_{q\omega}$ and $p \mid Y_{q\omega}$ (by (6)). Putting $n = r$ and $m = q\omega$ in (8), we see that

$$A_\kappa \equiv X_{qw} A_r \pmod{p}.$$

By (7), we have $X_{q\omega}^3 \equiv P_3^{q\omega} \pmod{p}$; hence, $p \nmid X_{q\omega}$ and since $p \mid A_\kappa$, we get $p \mid A_r$ which contradicts the definition of ω unless $r = 0$. In this case, we have $\omega \mid \kappa$. It follows that p can only have a single rank of appearance in (A_n). □

We now deal with the case of $p \mid h(A_2)P_3$. We first require two simple lemmas.

Lemma 3. *If m is any positive integer and $m \mid h(A_2)$, then for all $n \geq 0$,*

$$A_n \equiv u_n(P_1 - k, k^2 - P_1 k + P_2) \pmod{m},$$

where k satisfies $f(k) \equiv 0 \pmod{m}$.

Proof. We have

$$h(P_1 - x) = -f(x).$$

Thus, if $m \mid h(A_2)$, then $A_2 \equiv P_1 - k \pmod{m}$, where $f(k) \equiv 0 \pmod{m}$. Let u_n denote the Lucas function $u_n(P_1 - k, k^2 - P_1k + P_2)$. It follows that the lemma holds for $n = 0$, 1, 2. Since

$$P_3 \equiv k(k^2 - P_1k + P_2) \pmod{m}, \tag{22}$$

we get

$$-ku_{n+2} \equiv -k(P_1 - k)u_{n+1} + P_3u_n \pmod{m}.$$

The lemma now follows by using (1) and induction on n. □

Lemma 4. *Suppose $m \mid P_3$. If $n \geq 2$,*

$$Z_n \equiv u_{n-1}(P_1, P_2), \quad Y_n \equiv -P_2u_{n-2}(P_1, P_2) \pmod{m}.$$

Proof. Follows easily on noting the initial conditions of (Y_n), (Z_n), observing (1) with $P_3 \equiv 0 \pmod{m}$, and using induction on n. □

We are now able to restrict p in the following result.

Lemma 5. *Suppose p is a prime such that $p \mid h(A_2)P_3$. If $p \mid A_n$ and $p \mid P_3$, then $p \mid h(A_2)$.*

Proof. Suppose $p \nmid h(A_2)$. By Theorem 1, we must have $p \mid Z_n$. Since $p \mid A_n$, we must have $n \geq 2$ and $p \mid u_{n-1}(P_1, P_2)$ by Lemma 4. Also, by (6) we get $p \mid Y_n$ and by Lemma 4 we get $p \mid P_2u_{n-2}(P_1, P_2)$. If $p \nmid P_2$, then $p \mid u_{n-1}(P_1, P_2)$ and $p \mid u_{n-2}(P_1, P_2)$. By (20) we have

$$u_{n-1}^2(P_1, P_2) - u_{n-2}(P_1, P_2)u_n(P_1, P_2) = P_2^{n-2},$$

hence, $p \mid P_2$, a contradiction. Thus, $p \mid P_2$. By Lemma 1, we cannot have $p \mid P_1$, but

$$u_{n-1}(P_1, P_2) \equiv P_1^{n-2} \pmod{p}$$

which implies that $p \nmid u_{n-1}(P_1, P_2)$, a contradiction. □

We are now able to prove Lemma 6.

Lemma 6. *If p is a prime, $p \mid A_n$ and $p \mid h(A_2)$, then p must be monoapparitic in (A_n).*

Proof. By Lemma 3, we have

$$A_n \equiv u_n(P_1 - k, k^2 - P_1k + P_2) \pmod{p},$$

where $p \mid f(k)$. If $p \mid k^2 - P_1k + P_2$, then $u_n \equiv (P_1 - k)^{n-1} \pmod{p}$ which implies that $p \nmid A_n$ when $p \nmid P_1 - k$, a contradiction. If $p \mid P_1 - k$, then $p \mid P_2$ and $p \mid P_3$ by (22). Also, since $A_2 = P_1 - k$, we get $p \mid \gcd(A_2P_1, P_2, P_3)$, contradicting Lemma 1. Thus, since $p \nmid k^2 - P_1k + P_2$, we know that p is monoapparitic in $(u_n(P_1 - k, k^2 - P_1k + P_2))$ from the theory of Lucas sequences. Hence, p must be monoapparitic in (A_n). □

Theorem 6. *If p is any prime such that $p \mid A_n$ for some $n \geq 2$, then p must be monoapparitic in (A_n).*

Proof. We have shown that if $p \mid P_3h(A_2)$, then p must be monoapparitic in (A_n). Combining this with Theorem 5, we see that all primes p which divide any A_n with $n \geq 2$ must be monoapparitic in (A_n). □

We conclude this section with the following results concerning (A_n).

Proposition 2. *If n, $m > 0$ and $\gcd(n, m) = 1$, then $\gcd(A_n, A_m) = 1$.*

Proof. Let $g = \gcd(A_n, A_m)$ and let p be any prime divisor of g. By Theorem 6 we know that p must be monoapparitic in (A_n), and if $\omega = \omega(p)$, then $\omega \mid n$ and $\omega \mid m$. Hence $\omega = 1$, which is impossible. □

6. Application of Hall's Method

Unfortunately, the above results are still not sufficient to deduce the precise form of (A_n). We can, however, use an idea of Hall [6] to restrict (A_n) further. We first require some lemmas, the first of which is [6, Lemma 1].

Lemma 7. *If $p \mid P_3$ and $p \mid A_n$, then n has a factor h such that $1 < h \leq \bar{n}$, where $\bar{n}$ is a fixed integer.*

Proof. Suppose p is any prime such that $p \mid P_3$ and $p \mid A_n$. By Lemma 5 we know that $p \mid h(A_2)$. In the proof of Lemma 6 we showed that

$$A_n \equiv u_n(P_1 - k, k^2 - P_1k + P_2) \pmod{p},$$

where $p \mid f(k)$ and $p \nmid k^2 - P_1k + P_2$. By (22), this means that $p \mid k$ and therefore

$$A_n \equiv u_n(P_1, P_2) \pmod{p}.$$

If $p \mid P_2$, then $p \mid P_1$ by (14), which by Lemma 1 contradicts the definition of (A_n). Thus we may assume that $p \nmid P_2$. By the theory of Lucas sequences, this means that $\omega(p) \mid p - \epsilon$, where $\epsilon = (D|p)$ and $D = P_1^2 - 4P_2$. Since $P_3 \neq 0$, there are only a fixed number of primes p such that $p \mid P_3$ and for each of these $1 < \omega(p) \leq p + 1 \leq P_3 + 1$. Thus, the lemma follows on putting $\bar{n} = P_3 + 1$. □

We also have a somewhat more general result than [6, Lemma 2].

Lemma 8. *Let K be any fixed non-zero integer. If $p \mid A_n$ and $p \mid K$, then n has a factor h (> 1) less than a finite limit $\bar{n} = \bar{n}(K)$.*

Proof. If $p \mid P_3$, then Lemma 7 proves this. If $p \nmid P_3$, we know by Theorem 4 that $\omega(p)$ exists and $\omega(p) \mid n$ by Theorem 6. Also, since $A_1 = 1$, we have $\omega(p) > 1$. Since $K \neq 0$, it has only a finite number of divisors; thus,

$$\bar{n} = \bar{n}(K) = 1 + \max\{\omega(p) : p \mid K\}$$

is a fixed integer, and there must exist some h such that $h > 1$, $h < \bar{n}$ and $h \mid n$. □

We will now assume that

$$f(x) = (x - r)(x^2 - sx + t),$$

where $r, s, t \in \mathbb{Z}$ and $x^2 - sx + t$ is irreducible over $\mathbb{Q}$, i.e., $d = s^2 - 4t$ is not a perfect square $(d \neq 0)$. Let β, γ be the roots of $x^2 - sx + t = 0$. Note that

$$P_1 = r + s, \quad P_2 = rs + t, \quad P_3 = rt, \quad \text{and} \quad \Delta = d(r^2 - sr + t)^2 \neq 0. \tag{23}$$

Since $P_3 \neq 0$, we must have $rtd \neq 0$. Also, if $s = 0$, then $\beta/\gamma = -1$ and $f(x)$ is degenerate, a case we exclude. Thus, $s \neq 0$ and we need only consider $rstd \neq 0$. Our aim is to provide evidence that strongly suggests that (A_n) must be either a Lucas function or the square of a Lehmer function.

Put

$$r = \alpha, \quad v_n = v_n(s,t) = \beta^n + \gamma^n, \quad \text{and} \quad u_n = u_n(s,t) = \frac{\beta^n - \gamma^n}{\beta - \gamma}.$$

Observe that

$$v_2 - 2r^2 + (2r - s)u_2 = -2(r^2 - rs + t) \neq 0.$$

Next, consider

$$H_n = \frac{v_n - 2r^n + (2r - s)u_n}{v_2 - 2r^2 + (2r - s)u_2}.$$

We see that $H_0 = 0 = Z_0$, $H_1 = 0 = Z_1$, $H_2 = 1 = Z_2$. Since H_n has the form (2), it must satisfy (1); thus, $Z_n = H_n$ and

$$Z_n = \frac{v_n - 2r^n + (2r - s)u_n}{v_2 - 2r^2 + (2r - s)u_2}. \tag{24}$$

Furthermore, if

$$J_n = (A_2 - s)Z_n + u_n,$$

then J_n also satisfies (1) and $J_0 = 0 = A_0$, $J_1 = u_1 = 1 = A_1$, and $J_2 = A_2$. Thus, $A_n = J_n$ and

$$A_n = (A_2 - s)Z_n + u_n. \tag{25}$$

By (24), (25), and (21), we find that

$$A_{n+p^2-1} \equiv A_n \pmod{p} \quad (n \geq 0)$$

for any odd prime p such that $p \nmid P_3\Delta$. In this case we have $\omega(p) \mid p^2 - 1$. Also, the next lemma permits us to assume in what follows that $h(A_2) \neq 0$.

Lemma 9. *If $h(A_2) = 0$, then $A_n = u_n$, and therefore (A_n) is a Lucas sequence.*

Proof. If $h(A_2) = 0$, we have $f(P_1 - A_2) = 0$ which implies that $P_1 - A_2 = r$. By the first formula of (23), this means that $A_2 = s$. The lemma now easily follows from (25). □

We now have a result like [6, Lemma 3].

Lemma 10. *If q is a sufficiently large prime, then $A_q^2 \equiv 1 \pmod{q}$.*

Proof. By Lemma 7, A_q has no prime factor dividing P_3. If $p \mid A_q$, then $\omega(p) \mid q$ and since $\omega(p) > 1$, we get $\omega(p) = q$. By Lemma 8 we see that for $K = \Delta$, we cannot have $p \mid \Delta$. Hence, $\omega(p) \mid p^2 - 1$ and $q \mid p^2 - 1$. Since $p^2 \equiv 1 \pmod{q}$ for every prime p dividing A_q, it follows by multiplication that $A_q^2 \equiv 1 \pmod{q}$. □

Now by Lemma 10, we have

$$A_q^2 \equiv 1 \pmod{q}$$

for all primes sufficiently large. Thus, again following Hall, we can prove the following lemma.

Lemma 11. *For the c_1, c_2, and c_3 in (2), we must have*

$$c_1 + c_2 + c_3 = 0,$$
$$c_1\alpha + c_2\beta + c_3\gamma = 1,$$

and

$$c_1\alpha + c_2\gamma + c_3\beta = \epsilon,$$

where $\epsilon^2 = 1$.

Proof. Note that since $A_0 = 0$ and $A_1 = 1$ we have $c_1 + c_2 + c_3 = 0$ and $c_1\alpha + c_2\beta + c_3\gamma = 1$. Now, for all sufficiently large primes q such that $(d/q) = -1$ (since d is

not a perfect square, there must exist infinitely many q such that $(d/q) = -1$), we have $A_q^2 \equiv A_1^2 \pmod{q}$, thus

$$(c_1\alpha^q + c_2\beta^q + c_3\gamma^q)^2 \equiv (c_1\alpha + c_2\beta + c_3\gamma)^2 \pmod{q}. \tag{26}$$

In our case $f(x) = (x - r)(x^2 - sx + t)$ where $\alpha = r \in \mathbb{Z}$; consequently, we have

$$\alpha^q \equiv \alpha, \quad \beta^q \equiv \gamma, \quad \text{and} \quad \gamma^q = \beta \pmod{\mathfrak{q}}$$

where $\mathfrak{q}$ is a prime ideal dividing q in $\mathbb{Q}(\beta, \gamma) = \mathbb{Q}(\sqrt{d})$. Hence from (26)

$$(c_1\alpha + c_2\gamma + c_3\beta)^2 \equiv (c_1\alpha + c_2\beta + c_3\gamma)^2 \pmod{\mathfrak{q}}.$$

Since $c_1\alpha + c_2\beta + c_3\gamma = 1$, we get

$$(c_1\alpha + c_2\gamma + c_3\beta)^2 \equiv 1 \pmod{\mathfrak{q}}. \tag{27}$$

Since the difference of the two sides of (27) is an algebraic number divisible by infinitely many distinct prime ideals, it must be zero, so $c_1\alpha + c_2\gamma + c_3\beta = \epsilon = \pm 1$. □

We now deal separately with the cases of $\epsilon = -1$ and $\epsilon = 1$.

7. The Case of $\epsilon = -1$

When $\epsilon = -1$, we get

$$c_2(\beta - \alpha) + c_3(\gamma - \alpha) = 1 \tag{28}$$

and

$$c_2(\gamma - \alpha) + c_3(\beta - \alpha) = -1. \tag{29}$$

Thus,

$$c_2 = \frac{\begin{vmatrix} 1 & \gamma - \alpha \\ -1 & \beta - \alpha \end{vmatrix}}{e} \quad \text{and} \quad c_3 = \frac{\begin{vmatrix} \beta - \alpha & 1 \\ \gamma - \alpha & -1 \end{vmatrix}}{e},$$

where

$$e = \begin{vmatrix} \beta - \alpha & \gamma - \alpha \\ \gamma - \alpha & \beta - \alpha \end{vmatrix} = (\beta - \alpha)^2 - (\gamma - \alpha)^2 = (\beta - \gamma)(\beta + \gamma - 2\alpha).$$

If $\beta + \gamma \neq 2\alpha$, then $e \neq 0$ and

$$c_2 = \frac{1}{\beta - \gamma}, \quad c_3 = -\frac{1}{\beta - \gamma}, \quad \text{and} \quad c_1 = 0.$$

Here $A_n = \dfrac{\beta^n - \gamma^n}{\beta - \gamma} = u_n(s,t)$, a Lucas function. Also, from (23) and (13), we see that this (A_n) satisfies (1).

We next deal with the case of $\epsilon = -1$, $2\alpha = \beta + \gamma$, and $h(A_2) \neq 0$. Since $s = 2r$, we get

$$P_1 = 3r, \quad P_2 = 2r^2 + t, \quad P_3 = rt,$$

and $d = s^2 - 4t = 4(r^2 - t)$. By (24), we also get

$$Z_n = \frac{v_n - 2r^n}{v_2 - 2r^2},$$

where

$$v_2 - 2r^2 = s^2 - 2t - 2r^2 = s^2/2 - 2t = d/2 \neq 0.$$

By Theorem 1, we must have

$$A_n \mid h(A_2) \left(\frac{v_n - 2r^n}{d/2} \right)^2; \quad \text{thus,} \quad A_n \mid h(A_2)(v_n - 2r^n)^2.$$

Now let p be any prime such that $p \mid A_n$ and $p \nmid h(A_2)$. We must have $p \mid v_n - 2r^n$. Also, since p must also divide Z_n, we see by (25) that $p \mid u_n$. Hence, by (15) we get

$$v_n^2 \equiv 4t^n \pmod{p}.$$

Also, since $v_n \equiv 2r^n \pmod{p}$, we have

$$v_n^2 \equiv 4r^{2n} \pmod{p}.$$

Thus,

$$p \mid 4(r^{2n} - t^n).$$

Let $w_n = w_n(r,t) = r^{2n} - t^n$. We have the following simple result.

Lemma 12. *If $\tau = \tau(p)$ is the least positive integer such that $p \mid w_\tau$, then when $p \nmid (r^2 - t)rt$, τ exists, $\tau > 1$, and $\tau \mid p - 1$.*

Proof. On noting that

$$w_n = r^{2n} - t^n = \frac{((r^2)^n - t^n)}{(r^2 - t)} \cdot (r^2 - t) = (r^2 - t)u_n(r^2 + t, r^2 t),$$

this result follows from Theorems 2 and 3. Notice that the discriminant here is $(r^2 - t)^2$. □

Let $K = (r^2 - t)rt$ $(\neq 0)$ and q be any prime such that $q > \bar{n}(K)$. Observe that $2 \mid K$. By Lemma 8 we see that if p is any prime divisor of A_q, then $p \nmid K$. Also, $p \mid w_q$ means that $\tau(p) \mid q$, implying $\tau(p) = q$. Since $\tau(p) \mid p - 1$, we get

$p \equiv 1 \pmod{q}$; it follows that $A_q \equiv 1 \pmod{q}$. Since $A_q \equiv 1 \pmod{q}$ for all sufficiently large primes q, we must, by the reasoning employed in the proof of Lemma 11 find that

$$c_1\alpha + c_2\gamma + c_3\beta = 1.$$

But this implies $\epsilon = 1$, a contradiction. It follows that if $\epsilon = -1$, then (A_n) can only be a Lucas sequence (u_n).

8. The Case of $\epsilon = 1$

If $\epsilon = 1$, then from Lemma 11

$$c_2(\beta - \alpha) + c_3(\gamma - \alpha) = 1$$

and

$$c_2(\gamma - \alpha) + c_3(\beta - \alpha) = 1.$$

By adding, we get

$$(c_2 + c_3)(\beta + \gamma - 2\alpha) = 2.$$

Thus, $2r - s = 2\alpha - \beta - \gamma \neq 0$ which implies that $e \neq 0$ and so

$$c_2 = \frac{\begin{vmatrix} 1 & \gamma - \alpha \\ 1 & \beta - \alpha \end{vmatrix}}{e} = \frac{1}{\beta + \gamma - 2\alpha} \quad \text{and} \quad c_3 = \frac{\begin{vmatrix} \beta - \alpha & 1 \\ \gamma - \alpha & 1 \end{vmatrix}}{e} = \frac{1}{\beta + \gamma - 2\alpha}.$$

Thus, $c_1 = -2c_2$, and consequently

$$A_n = \frac{2\alpha^n - \gamma^n - \beta^n}{2\alpha - \gamma - \beta} = \frac{2r^n - v_n(s,t)}{2r - s}. \tag{30}$$

Since $A_2 \in \mathbb{Z}$, we must have

$$2r - s \mid 2r^2 - v_2(s,t).$$

Thus,

$$2r - s \mid 2r^2 - s^2 + 2t.$$

Since $4r^2 - 2s^2 + 4t = 4r^2 - s^2 - d = (2r - s)(2r + s) - d$, we find that $2r - s \mid d$.

Since we must have $A_n \mid A_{2n}$ (for all $n > 0$), we get

$$2r^n - v_n(s,t) \mid 2r^{2n} - v_{2n}(s,t).$$

Also, by (16), $v_{2n} = v_n^2 - 2t^n$; hence,

$$2r^n - v_n(s,t) \mid 2r^{2n} - v_n^2 + 2t^n. \tag{31}$$

Since $2r^{2n}-v_n^2+2t^n = -2r^{2n}+4r^{2n}-v_n^2+2t^n = -2(r^{2n}-t^n)+(2r^n-v_n)(2r^n+v_n)$, we have

$$2r^n - v_n(s,t) \mid 2(r^{2n}-t^n) \quad \text{for all} \quad n>0.$$

Hence

$$A_n \mid \frac{2(r^{2n}-t^n)}{2r-s} \quad \text{for all} \quad n>0. \tag{32}$$

Since $A_n = \dfrac{2r^n - v_n}{2r-s}$, we must have

$$2r^n - v_n \mid 2w_n \quad \text{for every } n>0. \tag{33}$$

By (15) we have

$$v_n^2(s,t) - du_n^2(s,t) = 4t^n;$$

hence, from (31) and (32), we find that

$$(2r-s)A_n \mid du_n^2(s,t)$$

or

$$A_n \mid \frac{d}{2r-s}u_n^2(s,t). \tag{34}$$

We next deal with a case where we find that (A_n) can be a divisibility sequence. Suppose $r^2 = t$. Here we have

$$P_1 = r+s, \quad P_2 = r(r+s), \quad P_3 = r^3, \quad \text{and} \quad A_2 = 2r+s.$$

Let u_n denote $u_n(\sqrt{2r+s}, r)$, which is essentially (except for a constant multiple which depends only on the parity of n) a Lehmer function (see Section 4). Suppose for some $n \geq 0$, we have

$$A_n = u_n^2, \quad A_{n+1} = u_{n+1}^2, \quad \text{and} \quad A_{n+2} = u_{n+2}^2. \tag{35}$$

This is certainly true for $n=0$. We have

$$A_{n+3} = P_1u_{n+2}^2 - P_2u_{n+1}^2 + P_3u_n^2.$$

Since

$$u_{n+2} = \sqrt{2r+s}u_{n+1} - ru_n,$$

we have

$$ru_n = \sqrt{2r+s}u_{n+1} - u_{n+2},$$

and therefore

$$r^3u_n^2 = r(2r+s)u_{n+1}^2 - 2r\sqrt{2r+s}u_{n+1}u_{n+2} + ru_{n+2}^2.$$

Thus,

$$\begin{aligned} P_1u_{n+2}^2 - P_2u_{n+1}^2 + P_3u_n^2 & \\ &= P_1u_{n+2}^2 - P_2u_{n+1}^2 + r(2r+s)u_{n+1}^2 - 2r\sqrt{2r+s}u_{n+1}u_{n+2} + ru_{n+2}^2 \\ &= (2r+s)u_{n+2}^2 - 2r\sqrt{2r+s}u_{n+1}u_{n+2} + r^2u_{n+1}^2 \\ &= (\sqrt{2r+s}u_{n+2} - ru_{n+1})^2 \\ &= u_{n+3}^2. \end{aligned}$$

Hence $A_{n+3} = u_{n+3}^2$. Thus, by induction, we have $A_n = u_n^2$ for $n \geq 0$.

This means that if $r^2 = t$, we are done with the $\epsilon = 1$ case. We next consider the more difficult case of $r^2 \neq t$.

9. The Case of $\epsilon = 1$ and $t \neq r^2$

Most of what we have discussed so far would have been known to or deduced by Ward. However, when we reach the case of $\epsilon = 1$ with $t \neq r^2$, our approach must become much more speculative. It is certainly conceivable that Ward believed that no DS could exist in this case, but we have few ideas concerning how or if he proved this. In view of his apparent reticence regarding this issue, it is likely that he did not have a complete proof. In what follows we look at how he might have approached this problem.

Recapitulating, in this case we have $P_1 = r + s$, $P_2 = rs + t$, and $P_3 = rt$ for nonzero integers r, s, and t, where $d = s^2 - 4t$ is not a perfect square and $2r - s \neq 0$. Furthermore, $(2r - s) \mid d$ and $s \equiv d' \pmod 2$, where $d' = d/(2r - s)$. It is not unreasonable to assume for this discussion, as did Hall, that $\gcd(P_2, P_3) = 1$. This means that $\gcd(r, t) = \gcd(s, t) = 1$. Let $\mathcal{T}$ denote any triple of integers (r, s, t) satisfying these above conditions. We have $A_2 = (2r + (s - d'))/2$ and, more generally, $A_n = (2r^n - v_n(s, t))/(2r - s)$. Ward was undoubtedly struck by his (likely) discovery that of all possible third-order linear recurrences, only the above candidate for (A_n) could be a DS distinct from a Lucas sequence or the square of a Lehmer sequence. He was also very aware of the divisibility properties of second-order sequences like the Lucas sequences and of third-order recurrence sequences like (A_n) (see Ward [11, 12, 15]). We now need to investigate the possible existence of any $\mathcal{T}$ for which the corresponding (A_n) is a DS. We will say that such a $\mathcal{T}$ is *admissible*. In what follows we will attempt to show why it is very unlikely that any admissible $\mathcal{T}$ exists.

We next establish the following simple results. Let r, t, s, and d be defined as above and put $K = rt(r^2 - t)d$.

Theorem 7. *If for the DS (A_n) corresponding to a given $\mathcal{T}$, we have a prime p such that $p \mid A_n$ for some $n > 0$ and $p \nmid K$, then $\lambda(p) \mid n$, where $\lambda(p) = \operatorname{lcm}[\tau(p), \rho(p)]$.*

Proof. By (32) we must have $p \mid w_n(r,t)$, which by lemma 12, means that $\tau(p) \mid n$. Also, by (34), we must have $p \mid u_n(s,t)$, which means by Theorem 3 that $\rho(p) \mid n$. It follows easily that $\lambda(p) \mid n$. □

Corollary 1. *Let $\omega(p)$ be the rank of appearance of a prime p in (A_n). Under the conditions of the theorem, we have $\omega(p) = \kappa\lambda(p)$, where κ is an integer.*

Proposition 3. *Let p be an odd prime such that $p \nmid 2r - s$ and $n > 0$. If $p \mid u_n$ and $p \mid w_n$, then $p \mid A_{2n}$.*

Proof. From (15), we see that

$$v_n^2 - du_n^2 = 4t^n.$$

Since $p \mid u_n$ and $r^{2n} \equiv t^n \pmod{p}$, we get

$$v_n^2 \equiv 4r^{2n} \pmod{p}.$$

Thus, by (16) we have

$$v_{2n} \equiv 2r^{2n} \pmod{p},$$

and therefore $p \mid A_{2n}$ by (30). □

Corollary 2. *Let p be a prime such that $p \nmid K$ and put $\lambda = \lambda(p)$. Suppose (A_n) is a DS; then we have $\omega = \kappa\lambda$, where $\kappa = 1$ or 2.*

Proof. By the proposition we have $p \mid A_{2\lambda}$. Since $\lambda \mid \omega$ by Theorem 7 and $\omega \mid 2\lambda$ (Theorem 6), the result follows. □

Proposition 4. *Let p be a prime as defined in Theorem 7. If $p \mid A_n$ and $p \mid w_n$, then $\lambda \mid n$.*

Proof. Since $p \mid w_n$, we have $\tau \mid n$. By (30), we have $v_n \equiv 2r^n \pmod{p}$ and by (15)

$$du_n^2 \equiv 4(r^{2n} - t^n) \equiv 4w_n \pmod{p}.$$

Since $p \mid w_n$ and $p \nmid d$, we have $p \mid u_n$ which implies that $\rho \mid n$, and therefore $\lambda \mid n$. □

Thus, if for some prime p, the value of $\omega(p) \neq \lambda$ or 2λ, the corresponding $\mathcal{T}$ cannot be admissible. In this case we call the prime an *eliminator prime* for $\mathcal{T}$. A simple example of an eliminator prime for $\mathcal{T} = (r,s,t)$ is any odd prime p such that $p \mid rt$ and $p \mid A_n$. In this case we find by (32) that we must have $p \mid r^{2n} - t^n$, which means that $p \mid r$ and $p \mid t$, which is impossible. If $\mathcal{T} = (1,3,5)$, we find that $5 \mid A_3$ $(= -20)$, and therefore $p = 5$ is an eliminator prime for $\mathcal{T}$. Unfortunately, it is possible to find many examples of $\mathcal{T}$ where $p \mid rt$ and $\omega = \omega(p)$ does not exist. For consider the case of $p \mid r$, $p \nmid d$, $p \not\equiv (d|p) \pmod{4}$, and $(t|p) = +1$. Here by

[1, Theorem 36] we see that $\rho(p)$ must be odd, which by [1, Theorem 19] means that $p \nmid v_n(s,t)$ and therefore $p \nmid A_n$ for any $n > 0$. A simple instance of this is provided by $\mathcal{T} = (5,6,1)$ with $p = 5$. Nevertheless, in this case we have $A_3 = 13$ and $13 \nmid u_3(6,1)$ $(= 35)$. Thus, by (34), 13 is an eliminator prime for this (A_n).

If a prime p is such that $p \nmid K$, then by Theorem 4, $\omega(p)$ must exist, and by Proposition 4 we see that p is an eliminator prime when $p \nmid w_\omega$ or $\tau(p) \nmid \omega$. Similarly, p is an eliminator prime if $p \nmid u_\omega$ or $\rho(p) \nmid \omega$. For example, if $\mathcal{T} = (1,3,5)$, then $A_4 = -51$ and $\omega(17) = 4$. However, $\tau(17) = 16$; thus, 17 is an eliminator prime for $\mathcal{T}$. Also, $u_4(3,5) = -3$ and $\rho(17) = 18$. Indeed, since for a given $\mathcal{T}$, the two sequences $(u_n(s,t))$ and $(u_n(r^2+t, r^2t))$ have discriminants which are distinct—one is not a square and the other is a perfect integral square—and are independent of each other, it is very likely that for an infinitude of values $m \geq 2$, we would expect that

$$g_m(r,s,t) = \gcd(u_m(s,t), u_m(r^2+t, r^2t))$$

would be small with respect to the values of $u_m(s,t)$ and $u_m(r^2+t, r^2t)$ and frequently be 1. This would particularly be the case when m is a prime because the possible prime divisors of $u_m(s,t)$ and $u_m(r^2+t, r^2t)$ are greatly restricted to those with ranks of appearance in the respective sequences equal to m. By Theorems 2 and 3 this means that any prime divisor of $u_m(s,t)$ must be of the form $km \pm 1$ and any prime divisor of $u_m(r^2+t, r^2t)$ must be of the form $km+1$, but in view of the distinctness of the arguments of g_m, it seems most improbable that the same prime of the form $km+1$ would divide both of them.

By Lemma 8, with $K = rtd(r^2-t)$, we know that for a sufficiently large prime q, we have some prime divisor p of A_q such that p does not divide K. Furthermore, we might reasonably anticipate that this p also would not divide $g_q(r,s,t)$. Of course, by (32) and (34) this means that p must be an eliminator prime for $\mathcal{T}$.

We can also approach the problem of finding an eliminator prime for a given $\mathcal{T}$ from a somewhat different direction. Suppose q is an odd prime and that p is some prime divisor of A_{q^m} $(m \geq 1)$. We note that since $\omega(p) \mid q^m$ and $A_1 = 1$, we must have $\omega(p) = q^k$ $(1 \leq k \leq m)$. Also, if $p \nmid K$, we know that $\tau(p)$ and $\rho(p)$ must exist and $\tau(p)$, $\rho(p) > 1$. In addition, we know that since $q^k = \omega(p) = \kappa\lambda(p)$, we can only have $\kappa = 1$. Since d is not a perfect square, there is no a priori reason to expect that $(d|p)$ can only be 1, so we may assume for the sake of argument that $\varepsilon = (d|p) = -1$. Let $g = \gcd(\tau(p), \rho(p))$. Since $\tau(p) \mid p-1$ and $\rho(p) \mid p-\varepsilon$, we can only have $g = 1$ or 2. Since $g \mid \lambda(p)$, and $\lambda(p)$ is odd, we have $g = 1$ and $q^k = \lambda(p) = \tau(p)\rho(p)$, which means that one of $\tau(p)$ or $\rho(p)$ is 1, an impossibility. We have proved the following result.

Theorem 8. *For a given $\mathcal{T}$, the corresponding sequence (A_n) cannot be a divisibility sequence when, for any prime q, there exists some prime divisor p of A_{q^m} $(m \geq 1)$ such that $p \nmid K$ and $(d|p) = -1$.*

For example, consider $\mathcal{T} = (1, 3, 4)$. We have $d = -7$, $A_{11} = 395 = 5 \cdot 79$, and $5 \nmid rtd(r^2 - t)d$. Since $(-7|5) = -1$, we see that 5 is an eliminator prime for $\mathcal{T}$.

By Proposition 2 we know that all the prime divisors of A_q must be distinct from those of $A_{q'}$, when q' is any sufficiently large prime distinct from q. For each sufficiently large prime q_i $(i = 1, 2, \ldots, k)$, let E_i denote the event that the prime $p_i \mid A_{q_i}$ and $(d|p_i) = 1$. Under the reasonable assumption that the events E_i and E_j are independent for distinct q_i and q_j and that the probability of each E_i is $1/2$, we find the probability that some $p_i \mid A_{q_i}$ $(i = 1, 2, \ldots, k)$ with $(d|p_i) = -1$ is $1 - (1/2)^k$. Thus, we would expect that it is always possible to find an eliminator prime for $\mathcal{T}$ after only a few trials at q_1, q_2, ..., etc.

Another means of determining eliminator primes for a given $\mathcal{T}$ can be derived from the following proposition:

Proposition 5. *Suppose p and π are primes such that $\pi^\nu \,||\, p - 1$ and $\nu \geq 1$. If $p \mid A_n$ and*

$$p \nmid w_{\frac{p-1}{\pi^\mu}} \tag{36}$$

for some μ such that $1 \leq \mu \leq \nu$, then $\pi \mid n$.

Proof. Put $\tau = \tau(p)$. We must have $\tau \mid p - 1$ and by (36) we must also have $\tau \nmid (p - 1)/\pi^\mu$. It follows that $\pi \mid \tau$. Since $p \mid A_n$, we get $\tau \mid n$ and the result follows. □

Corollary 3. *Suppose p and π are primes satisfying the conditions of Proposition 5. If $p \mid A_n$ and $\pi \nmid n$, then p is an eliminator prime for $\mathcal{T}$ when (36) holds.*

Consider the case of $\pi = 2$ and $\mu = 1$ in Corollary 3. We find that if $(t|p) = -1$, then p is an eliminator prime for $\mathcal{T}$ when n is odd. This suggests that if t is not a perfect square and p is any odd prime divisor of A_n, where n is odd, the probability that p is an eliminator prime for $\mathcal{T}$ is about $1/2$. For example, for $r = 1$, $s = 3$, and $t = 5$, we get $A_{13} = -9359 = -7^2 \cdot 191$. Thus, for $p = 7$, we have $(5|7) = -1$ and 7 must be an eliminator prime for $\mathcal{T} = (1, 3, 5)$. Also, since 13 and 17 divide $A_{15} = 349180$, we see that both of these primes are also eliminator primes for $\mathcal{T}$. If $r = 1$, $s = 3$, $t = 4$, then t is a perfect square, but in this case $A_7 = 85 = 5 \cdot 17$ and since

$$4^{(17-1)/8} \not\equiv 1 \pmod{17},$$

we see by Corollary 3, with $\pi = 2$ and $\mu = 3$, that 17 is an eliminator prime for $\mathcal{T} = (1, 3, 4)$.

In an attempt to find an admissible $\mathcal{T}$, we programmed a computer to conduct a search over various ranges of values r, s, t. However, these searches were, of course, all fruitless because for each candidate $\mathcal{T}$, the computer found a small (usually at most 29) eliminator prime after only a few trials for p. Indeed, the average number of such trials was only slightly in excess of 3. Suppose we consider a fixed value

for P_3. Clearly, there can only be a finite number of integer pairs (r,t) such that $rt = P_3$ and $\gcd(r,t) = 1$. Furthermore, since $(2r-s) \mid (s^2-4t)$, we find that $(2r-s) \mid 4(r^2-t)$. Thus, since $r^2 - t \neq 0$, there can only be a finite number of integers r, s, and t such that $\mathcal{T} = (r,s,t)$ is a triple corresponding to (A_n) for a given P_3. It seems that it is always a straightforward matter, using our previous results, like Theorem 8, to show that such $\mathcal{T}$s are inadmissible. For example, for $|P_3| \leq 50$, we used a computer to eliminate all such $\mathcal{T}$s. Thus, if $|P_3| \leq 50$, we can use our simple methods to show that (A_n) cannot be a divisibility sequence.

Initially, the above or similar heuristic deliberations might have convinced Ward that (A_n) could not be a DS when $r^2 \neq t$, and this possibly inspired his comment to Hall. However, it appears that he must have realized later that he didn't have a complete proof of his result, which explains his subsequent silence.

References

[1] C. J.-C. Ballot and H. C. Williams, *The Lucas Sequences: Theory and Applications*, CMS/CAIMS Books in Mathematics, Vol. 8, Springer Nature, Switzerland AG, 2023.

[2] E. T. Bell, Notes on recurring series of the third order, *Tohoku Math. J.* **24** (1924), 168-184.

[3] F. Beukers, The zero-multiplicity of ternary recurrences, *Compos. Math.* **77** (1991), 165–177.

[4] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs **104**, AMS, Providence RI, 2003.

[5] A. Granville, Classifying linear division sequences, *Amer. J. Math.*, to appear. Available at: `https://arxiv.org/abs/2206.11823`.

[6] M. Hall Jr., Divisibility sequences of third order, *Amer. J. Math.* **58** (1936), 577-584.

[7] M. Hall Jr., An isomorphism between linear recurring sequences and algebraic rings, *Trans. Amer. Math. Soc.* **44** (1938), 196–218.

[8] D. H. Lehmer, An extended theory of Lucas' functions, *Ann. of Math.* **31** (1930), 419-448.

[9] K. Mahler, Eine arithmetishe Eigenschaft der Taylor-Koeffizienten rationaler Funktionen, *Proc. Amsterdam Acad.* **38** (1935), 50–60.

[10] P. Ribenboim, *The Little Book of Big Primes*, 2nd ed., Springer, NY, 2004.

[11] M. Ward, The characteristic number of a sequence of integers satisfying a linear recursion relation, *Trans. Amer. Math. Soc.* **33** (1931), 153–165.

[12] M. Ward, The distribution of residues in a sequence satisfying a linear recursion relation, *Trans. Amer. Math. Soc.* **33** (1931), 166–190.

[13] M. Ward, The arithmetic theory of linear recurring series, *Trans. Amer. Math. Soc.* **35** (1933), 600–628.

[14] M. Ward, Note on an arithmetical property of recurring series, *Math. Z.* **39** (1934), 212–214.

[15] M. Ward, An arithmetical property of recurring sequences of the second order, *Bull. Amer. Math. Soc.* **40** (1934), 825–828.

[16] M. Ward, The null divisors of a linear recurring series, *Duke Math. J.* **2** (1936), 472–476.

[17] M. Ward, Linear divisibility sequences, *Trans. Amer. Math. Soc.* **41** (1937), 276–286.

[18] M. Ward, The law of apparition of primes in a Lucasian sequence, *Trans. Amer. Math. Soc.* **44** (1938), 68–86.

[19] M. Ward, The law of apparition and repetition of primes in a cubic recurrence, *Trans. Amer. Math. Soc.* **79** (1955), 72–90.

[20] H. C. Williams, *Édouard Lucas and Primality Testing*, Wiley-Interscience, 1998.

[21] H. C. Williams and R. K. Guy, Odd and even linear divisibility sequences of order 4, *Integers* **15** (2015), #A33, 21 pp.