ODD AND EVEN LINEAR DIVISIBILITY SEQUENCES OF ORDER 4

H. C. Williams

R. K. Guy

Received: 1/9/14, Revised: 1/19/15, Accepted: 6/9/15, Published: 7/17/15

Abstract

A sequence of rational integers $\{A_n\}$ is said to be a divisibility sequence if $A_n \mid A_m$ whenever $n \mid m$ and $A_n \neq 0$. If the divisibility sequence also satisfies a linear recurrence relation, it is said to be a linear divisibility sequence of order r, where r is the degree of the characteristic polynomial of the recurrence. The best known example of such a sequence of order 2 is the Lucas sequence $\{u_n\}$. In an attempt to extend Lucas's theory to sequences of order 4, it becomes necessary to examine odd and even divisibility sequences. In this paper we produce some conditions under which certain divisibility sequences of order 4 will be either even or odd.

1. Introduction

Let p, $q \in \mathbb{C}$ and α, β be the zeroes of $x^2 - px + q \in \mathbb{C}[x]$. We define, for any $n \in \mathbb{Z}$,

$$u_n = u_n(p,q) = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ v_n = v_n(p,q) = \alpha^n + \beta^n.$$

When p, q are integers, both $u_n(p,q)$ and $v_n(p,q)$ are integers for all $n \geq 0$ and when p, q are coprime are called the Lucas functions. Also $u_0 = 0$, $u_1 = 1$, $v_0 = 2$, $v_1 = p$ and $\{u_n\}$, $\{v_n\}$ both satisfy the second order linear recurrence

$$A_{n+1} = pA_n - qA_{n-1}.$$

When $p = \sqrt{r}$, where $r \in \mathbb{Z}$, we find that if

$$\bar{u}_n = \bar{u}_n(r,q) := \begin{cases} u_n(\sqrt{r},q) & \text{when } 2 \nmid n \\ u_n(\sqrt{r},q)/\sqrt{r} & \text{when } 2 \mid n \end{cases}$$

and

$$\bar{v}_n = \bar{v}_n(r,q) := \begin{cases} v_n(\sqrt{r},q)/\sqrt{r} & \text{when } 2 \nmid n \\ v_n(\sqrt{r},q) & \text{when } 2 \mid n \end{cases}$$

then $\bar{u}_n$ and $\bar{v}_n$ are integers for all integers $n \geq 0$. Also

$$\bar{u}_0 = 0,\ \bar{u}_1 = 1,\ \bar{u}_2 = 1,\ \bar{u}_3 = r - q,\ \bar{v}_0 = 2,\ \bar{v}_1 = 1,\ \bar{v}_2 = r - 2q,\ \bar{v}_3 = r - 3q.$$

When $(r,q)=1$, $\bar{u}_n(p,q)$ and $\bar{v}_n(p,q)$ are called the Lehmer functions (see [2]).

Furthermore, both $\{\bar{u}_n\}$ and $\{\bar{v}_n\}$ satisfy the fourth order linear recurrence

$$A_{n+4}=(r-2q)A_{n+2}-q^2A_n.$$

In general, a **linear recurrence sequence of order** r over $\mathbb{Z}$ is a sequence $\{A_n\}\subseteq\mathbb{Z}$, where we have

$$A_{n+r}=T_1A_{n+r-1}-T_2A_{n+r-2}+T_3A_{n+r-3}-\cdots+(-1)^{r+1}T_rA_n$$

and $A_0,\ A_1,\ \ldots,\ A_{r-1},\ T_1,\ T_2,\ \ldots,\ T_r$ are given fixed integers with $T_r\neq 0$. The polynomial

$$G(x)=\sum_{i=0}^{r}(-1)^iT_ix^{r-i}$$

is the **characteristic polynomial** of $\{A_n\}$.

If $\{A_n\}$ is a linear recurrence sequence, we say that an integer $m\ (>1)$ is a **null divisor** (see Ward [10, 9]) of $\{A_n\}$ if, for some minimal $k>0$, we have $m\mid A_n$ for all $n\geq k$. If $\{A_n\}$ has a null divisor, it is said to be a **null sequence**. In what follows we shall be concerned only with **non null sequences**. For example, the condition that $(p,q)=1$ ensures that both $\{u_n(p,q)\}$ and $\{v_n(p,q)\}$ are non null sequences. Similarly, the condition that $(r,q)=1$ ensures that both $\{\bar{u}_n(r,q)\}$ and $\{\bar{v}_n(r,q)\}$ are non null sequences.

Now suppose that the characteristic polynomial $F(x)$ of $\{A_n\}$ is of even degree $2k$ and has $2k$ distinct zeroes

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k,\ \beta_1,\ \beta_2,\ \ldots,\ \beta_k$$

such that $\alpha_i\beta_i$ is the same fixed integer Q for $i=1,2,\ldots,k$. Notice that the Lucas functions, the Lehmer functions, and the suggested extensions of the Lucas functions mentioned in Roettger, Williams and Guy [6] all possess such a characteristic polynomial. Lucas pointed out in [3, eqn (50)] that

$$u_{-n}=-u_n/q^n,\quad v_{-n}=v_n/q^n$$

for all $n\in\mathbb{Z}$. By analogy to the definitions in the theory of functions, we could say that $\{u_n\}$ is an **odd recurrence** and that $\{v_n\}$ is an **even recurrence**. More generally, if $\{A_n\}$ has the characteristic polynomial described above, then we say that $\{A_n\}$ is **odd** when $A_{-n}=-A_n/Q^n$ for all $n\in\mathbb{Z}$ and $\{A_n\}$ is **even** when $A_{-n}=A_n/Q^n$ for all $n\in\mathbb{Z}$.

If $m,\ n\in\mathbb{Z}$ amd $m,\ n>0$, we say that a sequence $\{A_n\}$ is a linear divisibility sequence if $A_n\mid A_m$ whenever $n\mid m$ and $A_n\neq 0$. We mention that both $\{u_n(p,q)\}$ and $\{\bar{u}_n(r,q)\}$ are linear divisibility sequences of orders 2 and 4 respectively. We also point out that if $\{A_n\}$ is a divisibility sequence, then it is only of limited interest

(see Hall [1]) if $A_0 \neq 0$. Thus, we shall always assume that $A_0 = 0$ and with no loss of generality that $A_1 = 1$.

The purpose of this paper is to derive some conditions under which a non null divisibility sequence with characteristic polynomial $F(x)$ and $k = 2$ is either even or odd.

2. Some Elementary Observations Concerning Even and Odd $\{A_n\}$

Given the above conditions on $F(x)$, we know that any particular recurrence sequence $\{A_n\}$ which has $F(x)$ as its characteristic polynomial must have the form

$$A_n = c_1\alpha_1^n + c_2\beta_1^n + c_3\alpha_2^n + c_4\beta_2^n + \cdots + c_{2k-1}\alpha_k^n + c_{2k}\beta_k^n \quad (2.1)$$

where c_1, c_2, ..., c_{2k} are constants whose values depend on α_1, β_1, α_2, β_2, ..., α_k, β_k and the initial conditions A_0, A_1, A_2, ..., A_{k-1}. We will now derive criteria for $\{A_n\}$ to be either even or odd.

Put $v_n(i) = \alpha_i^n + \beta_i^n$, $u_n(i) = (\alpha_i^n - \beta_i^n)/(\alpha_i - \beta_i)$ and

$$D_1 = \begin{vmatrix} v_0(1) & v_0(2) & \cdots & v_0(k) \\ v_1(1) & v_1(2) & \cdots & v_1(k) \\ \cdots & \cdots & \cdots & \cdots \\ v_{k-1}(1) & v_{k-1}(2) & \cdots & v_{k-1}(k) \end{vmatrix}, \qquad D_2 = \begin{vmatrix} u_1(1) & u_1(2) & \cdots & u_1(k) \\ u_2(1) & u_2(2) & \cdots & u_2(k) \\ \cdots & \cdots & \cdots & \cdots \\ u_k(1) & u_k(2) & \cdots & u_k(k) \end{vmatrix}.$$

Note that if $\alpha_i + \beta_i = \alpha_j + \beta_j$ $(i \neq j)$, then since $\alpha_i\beta_i = \alpha_j\beta_j$ we must have $\alpha_i = \alpha_j$ or β_j, which by definition of $F(x)$ is impossible. Thus, if we put $\rho_i = \alpha_i + \beta_i$, we have $\rho_i \neq \rho_j$ when $i \neq j$. We will need the following simple result.

Theorem 2.1. *Under the conditions defining $F(x)$, we must have $D_1 \neq 0$, $D_2 \neq 0$.*

Proof. We first note that (see, for example, (4.2.36), (4.2.35) of Williams [11])

$$v_n(i) = \sum_{j=0}^{\lfloor n/2 \rfloor} (-1)^j \frac{n}{j} \binom{n-j-1}{j-1} Q^j \rho_i^{n-2j},$$

$$u_n(i) = \sum_{j=0}^{\lfloor (n-1)/2 \rfloor} (-1)^j \binom{n-j-1}{j} Q^j \rho_i^{n-2j-1}.$$

In both formulas the coefficients of the powers of ρ_i are independent of i. Thus, by multiplying rows of D_1 (or D_2) by the corresponding coefficients and subtracting, we get

$$D_1/2 = D_2 = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \rho_1 & \rho_2 & \cdots & \rho_k \\ \rho_1^2 & \rho_2^2 & \cdots & \rho_k^2 \\ \cdots & \cdots & \cdots & \cdots \\ \rho_1^{k-1} & \rho_2^{k-1} & \cdots & \rho_k^{k-1} \end{vmatrix} = \prod_{i \neq j} (\rho_i - \rho_j) \neq 0.$$

□

By (2.1) we have

$$A_n = \sum_{i=1}^{k} c_{2i-1}\alpha_i^n + \sum_{i=1}^{k} c_{2i}\beta_i^n.$$

If $\{A_n\}$ is even, then we have

$$\begin{aligned} A_{-n} = \sum_{i=1}^{k} c_{2i-1}\alpha_i^{-n} + \sum_{i=1}^{k} c_{2i}\beta_i^{-n} &= Q^{-n}\sum_{i=1}^{k}\left(c_{2i-1}\beta_i^n + c_{2i}\alpha_i^n\right) \\ &= Q^{-n}A_n = Q^{-n}\sum_{i=1}^{k}\left(c_{2i-1}\alpha_i^n + c_{2i}\beta_i^n\right). \end{aligned}$$

Hence, for all $n \in \mathbb{Z}$, we must have

$$\sum_{i=1}^{k}(\alpha_i^n - \beta_i^n)(c_{2i-1} - c_{2i}) = 0.$$

We can write this as

$$\sum_{i=1}^{k} u_n(i)(\alpha_i - \beta_i)(c_{2i-1} - c_{2i}) = 0$$

but since $D_2 \neq 0$, this means that

$$(\alpha_i - \beta_i)(c_{2i-1} - c_{2i}) = 0 \qquad (i = 1, 2, \ldots, k)$$

and $c_{2i-1} = c_{2i}$ $(i = 1, 2, \ldots, k)$. Similarly, if $\{A_n\}$ is odd, then we must have

$$\sum_{i=1}^{k} v_n(i)(c_{2i-1} + c_{2i}) = 0$$

for all $n \in \mathbb{Z}$. As $D_1 \neq 0$, we get

$$c_{2i-1} = -c_{2i} \qquad (i = 1, 2, \ldots, k).$$

Note that if $c_{2i-1} = c_{2i}$ $(i = 1, 2, \ldots, k)$, then $\{A_n\}$ is even, and if $c_{2i-1} = -c_{2i}$ $(i = 1, 2, \ldots, k)$, then $\{A_n\}$ is odd. Thus, we have proved the following theorem.

Theorem 2.2. *If $\{A_n\}$ has $F(x)$ as its characteristic polynomial, then $\{A_n\}$ is even if and only if $c_{2i-1} = c_{2i}$ $(i = 1, 2, \ldots, k)$, and $\{A_n\}$ is odd if and only if $c_{2i-1} = -c_{2i}$ $(i = 1, 2, \ldots, k)$.*

We will now restrict our attention to the case of $k = 2$. In this case we have

$$\rho_1 + \rho_2 = \alpha_1 + \beta_1 + \alpha_2 + \beta_2 = T_1$$

$$\rho_1\rho_2 = (\alpha_1+\beta_1)(\alpha_2+\beta_2) = \alpha_1\alpha_2+\alpha_2\beta_1+\alpha_1\beta_2+\beta_1\beta_2 =$$
$$T_2 - \alpha_1\beta_1 - \alpha_2\beta_2 = T_2 - 2Q$$

If we put $P_1 = T_1$, $P_2 = T_2 - 2Q$, then $F(x) = (x^2 - \rho_1 x + Q)(x^2 - \rho_2 x + Q)$ or

$$F(x) = x^4 - P_1x^3 + (P_2+2Q)x^2 - P_1Qx + Q^2 \tag{2.2}$$

and
$$A_{n+4} = P_1A_{n+3} - (P_2+2Q)A_{n+2} + P_1QA_{n+1} - Q^2A_n \tag{2.3}$$

where P_1, P_2, $Q \in \mathbb{Z}$. Of course, $F(x)$ is the characteristic polynomial for the sequences $\{U_n\}$ and $\{V_n\}$ of Williams and Guy [12, 13]. The discriminant D of $F(x)$ is given by

$$D = E\Delta^2Q^2 \tag{2.4}$$

where $\Delta = P_1^2 - 4P_2$, $E = (P_2+4Q)^2 - 4QP_1^2$. We also have the identity

$$\Delta P_1^2 + 4E = (P_1^2 - 2P_2 - 8Q)^2 \tag{2.5}$$

hence, Δ and E cannot both be negative. Also, if $D \neq 0$, we have

$$A_n = c_1\alpha_1^n + c_2\beta_1^n + c_3\alpha_2^n + c_4\beta_2^n. \tag{2.6}$$

Now suppose that $\{A_n\}$ is even. In this case we must have $c_1 = c_2$, $c_3 = c_4$ and

$$A_n = c_1(\alpha_1^n + \beta_1^n) + c_3(\alpha_2^n + \beta_2^n).$$

If $\{A_n\}$ is a divisibility sequence, we have $c_1 + c_2 + c_3 + c_4 = A_0 = 0$ and therefore $c_1 = -c_3$. Since $A_1 = 1$, we also have

$$1 = c_1\alpha_1 + c_2\beta_1 + c_3\alpha_2 + c_4\beta_2 = c_1(\alpha_1 + \beta_1 - \alpha_2 - \beta_2).$$

Hence

$$A_n = \frac{\alpha_1^n + \beta_1^n - \alpha_2^n - \beta_2^n}{\alpha_1 + \beta_1 - \alpha_2 - \beta_2}.$$

This is the function U_n in [12]. Indeed, as shown in [12], $\{U_n\}$ is a divisibility sequence. Thus we see that there is one and only one *even* divisibility sequence for a recurrence with characteristic polynomial (2.2).

We are left, then, with the problem of characterizing the odd divisibility sequences having characteristic polynomial (2.2). Certainly, odd divisibility sequences exist, as we have seen that both $\{u_n(p,q)\}$ and $\{\bar{u}_n(r,q)\}$ are odd. Also, if $P_1 = p^3/q - 2p$, $P_2 = p^4/q - 3p^2$, $Q = q$, $A_{-1} = -1/q$, $A_2 = p^3/q$, then $A_n = u_n(p,q)^3/q^{n-1}$ and $\{A_n\}$ is an odd divisibility sequence. An example of such a sequence occurs as A056570 in Sloane [7]. This sequence is mentioned as Case 3.5.2 in Oosterhout [4]. In [7] two other divisibility sequences are listed; in all of the fourth order divisibility sequences contained in [7], these two, A127595 and A215466, are the only interesting ones that are odd. (We exclude the Lucas and Lehmer sequences from consideration.)

We conclude this section by developing a simple criterion for determining whether $\{A_n\}$ is an odd divisibility sequence. We recall from [12] that the sequences $\{W_n\}$ and $\{U_n\}$ can be defined by

$$W_n + \rho_i U_n = \alpha_i^n + \beta_i^n \quad (i = 1, 2).$$

It is also convenient to define sequences $\{X_n\}$ and $\{Y_n\}$ satisfying

$$X_n + \rho_i Y_n = (\alpha_i^n - \beta_i^n)/(\alpha_i - \beta_i) \quad (i = 1, 2). \tag{2.7}$$

We have $X_0 = 0$, $Y_0 = 0$, $X_1 = 1$, $Y_1 = 0$, $X_2 = 0$, $Y_2 = 1$, $X_3 = -Q - P_2$, $Y_3 = P_1$. These are integer valued sequences when $n \geq 0$ and have (2.2) as their characteristic polynomial. We also have $X_{-n} = -X_n/Q^n$, $Y_{-n} = -Y_n/Q^n$. Now if $\{A_n\}$ is odd, then by Theorem 2.2, there exist constants γ_1 and γ_2 such that

$$\begin{aligned} A_n &= \gamma_1 \left(\frac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1} \right) + \gamma_2 \left(\frac{\alpha_2^n - \beta_2^n}{\alpha_2 - \beta_2} \right) \\ &= \gamma_1(X_n + \rho_1 Y_n) + \gamma_2(X_n + \rho_2 Y_n) \\ &= (\gamma_1 + \gamma_2)X_n + (\gamma_1\rho_1 + \gamma_2\rho_2)Y_n. \end{aligned}$$

Since $A_1 = 1$ we put $\gamma_1 + \gamma_2 = 1$ and $A_2 = \gamma_1\rho_1 + \gamma_2\rho_2$. Thus, if $\{A_n\}$ is an odd divisibility sequence, we must have

$$A_n = X_n + A_2 Y_n \tag{2.8}$$

but this is not sufficient to guarantee that $\{A_n\}$ is a divisibility sequence.

3. The Case Where $P_1 = 0$

It is by no means clear that any divisibility sequence $\{A_n\}$ with characteristic polynomial (2.2) must be either even or odd. In this section we completely characterize all the divisibility sequences $\{A_n\}$ which can occur with $P_1 = 0$. We will show that when $P_1 = 0$ it is possible to have a divisibility sequence $\{A_n\}$ which is neither even nor odd.

When $P_1 = 0$, we have $F(x) = x^4 + (P_2 + 2Q)x^2 + Q^2$. Without loss of generality we can put

$$\alpha_1 = \frac{\sqrt{-P_2} + \sqrt{-(P_2+4Q)}}{2},\ \beta_1 = \frac{\sqrt{-P_2} - \sqrt{-(P_2+4Q)})}{2},\ \alpha_2 = -\beta_1,\ \beta_2 = -\alpha_1.$$

Hence, by (2.6),

$$A_n = (c_1 + (-1)^n c_4)\alpha_1^n + (c_2 + (-1)^n c_3)\beta_1^n.$$

Also, since $A_0 = 0$, we have $c_1 + c_2 + c_3 + c_4 = 0$. If $2 \mid n$, then

$$A_n = A_2 \frac{\alpha_1^n - \beta_1^n}{\alpha_1^2 - \beta_1^2} = A_2 \bar{u}_n(-P_2, Q).$$

If $2 \nmid n$, then

$$A_n = (c_1 - c_4)\alpha_1^n + (c_2 - c_3)\beta_1^n.$$

Since $A_1 = 1$, we can solve for $c_1 - c_4$ and $c_2 - c_3$ in terms of A_{-1} and find that

$$A_n = \frac{\alpha_1^{n+1} - \beta_1^{n+1}}{\alpha_1^2 - \beta_1^2} - Q^2 A_{-1} \frac{\alpha_1^{n-1} - \beta_1^{n-1}}{\alpha_1^2 - \beta_1^2}.$$

Since $2 \mid n+1$ and $2 \mid n-1$, we can write this as

$$A_n = \bar{u}_{n+1}(-P_2, Q) - Q^2 A_{-1} \bar{u}_{n-1}(-P_2, Q).$$

In what follows we will use $\bar{u}_n$ and $\bar{v}_n$ to denote $\bar{u}_n(-P_2, Q)$, $\bar{v}_n(-P_2, Q)$ respectively. If $2 \nmid n$, it is easy to verify that

$$\begin{aligned} \bar{u}_{n+1} + Q\bar{u}_{n-1} &= \bar{u}_n, \\ \bar{u}_{n+1} - Q\bar{u}_{n-1} &= \bar{v}_n. \end{aligned}$$

It follows that

$$2A_n = (1 + QA_{-1})\bar{v}_n + (1 - QA_{-1})\bar{u}_n \tag{3.1}$$

whenever $2 \nmid n$. If we put $B_n = A_{2n+1}$, then

$$B_{n+2} = -(P_2 + 2Q)B_{n+1} - Q^2 B_n.$$

Thus, $\{B_n\}$ is a second order linear recurring sequence, and Ward [10] (also proved earlier by Pólya [5]) has shown that if such a sequence is not degenerate (in this case α_1^2/β_1^2 is not a root of unity), then $\{B_n\}$ has an infinitude of distinct prime divisors.

If we put $C_1 = 1 + QA_{-1}$, $C_2 = 1 - QA_{-1}$, then since $B_1 = -(P_2 + 2Q) - Q^2 A_{-1}$, we see that QC_1, $QC_2 \in \mathbb{Z}$. Let $C = \max\{2, |Q|, |QC_1|, |QC_2|\}$.

We have $2A_{2n+1} = C_1\bar{v}_{2n+1} + C_2\bar{u}_{2n+1}$ and it is easy to verify that

$$\begin{aligned} \bar{v}_{3(2n+1)} &= \bar{v}_{2n+1}(-P_2\bar{v}_{2n+1}^2 - 3Q^{2n+1}) \\ \bar{u}_{3(2n+1)} &= \bar{u}_{2n+1}(-P_2\bar{v}_{2n+1}^2 - Q^{2n+1}) \end{aligned}$$

hence $$A_{3(2n+1)} = -(P_2\bar{v}_{2n+1}^2 + Q^{2n+1})A_{2n+1} - Q^{2n+1}C_1\bar{v}_{2n+1}.$$

If $\{A_n\}$ is to be a divisibility sequence, we must have $A_{2n+1} \mid A_{3(2n+1)}$. Hence

$$A_{2n+1} \mid Q^{2n+1}C_1\bar{v}_{2n+1}.$$

We next suppose that C_1 and C_2 are nonzero and let p be a prime such that $p > C$ and $p \mid B_n$. Such a prime must exist by Ward's result. Since $p \nmid Q$ and $p \nmid QC_1$ and p is odd, we must have $p \mid \bar{v}_{2n+1}$, but since $p \mid QB_n$, we must also have $p \mid QC_2\bar{u}_{2n+1}$ and $p \mid \bar{u}_{2n+1}$. Since any common prime divisor of $\bar{v}_{2n+1}$ and $\bar{u}_{2n+1}$

must divide $2Q$, this is impossible. It follows that if $\{A_n\}$ is to be a divisibility sequence, we must have C_1 or $C_2 = 0$.

If $C_1 = 0$, then $A_{2n+1} = \bar{u}_{2n+1}$, $A_{2n} = A_2\bar{u}_{2n}$. We see that in this case $\{A_n\}$ is an odd divisibility sequence. If $C_2 = 0$, then $A_{2n+1} = \bar{v}_{2n+1}$, $A_{2n} = A_2\bar{u}_{2n}$. The sequence $\{A_n\}$ is a divisibility sequence, but because $A_{-(2n+1)} = A_{2n+1}/Q^{2n+1}$ and $A_{-2n} = -A_{2n}/Q^{2n}$, it is neither an odd nor an even divisibility sequence when $A_2 \neq 0$.

An example of such a sequence occurs as A005013 in [7], where $Q = -1$, $P_2 = -1$ and $A_n = L_n$ (the Lucas number) when $2 \nmid n$ and $A_n = F_n$ (the Fibonacci number) when $2 \mid n$.

If $A_2 = 0 = P_1$, then $\{A_n\}$ is the even divisibility sequence $\{U_n\}$.

If α_i^2/β_i^2 is a root of unity, then there are only finitely many possible prime divisors of B_n (see §6 of [10]). As this is a case of little interest to us, we exclude it from our study.

We have seen that it is possible to have a non null divisibility sequence with characteristic function $F(x)$ given by (2.2) which is neither even nor odd. In the next sections we will consider the possible existence of such divisibility sequences when $P_1 \neq 0$. It is useful at this point to define S and G to be those squarefree integers such that

$$\Delta = SV^2, \quad E = GU^2 \tag{3.2}$$

and U, $V \in \mathbb{Z}$.

4. Some Preliminary Results

We first discuss the conditions that are necessary and sufficient for $\{A_n\}$ to have no null divisors. The following result is a special case of more general work of Ward [8, 9].

Proposition 4.1. *The sequence $\{A_n\}$ will have no null divisors if and only if $(P_1, P_2, Q) = 1$, $(A_3, P_2, Q) = 1$ and $(A_2, A_3, Q) = 1$.*

Proof. If p is a prime and either $p \mid (P_1, P_2, Q)$ or $p \mid (A_3, P_2, Q)$ or $p \mid (A_3, A_3, Q)$, then it is easy to see from (2.3) that $p \mid A_n$ for $n \geq 4$ in the first case, $p \mid A_n$ for $n \geq 3$ in the second case and $p \mid A_n$ for $n \geq 2$ in the last case. Thus in any of these cases p is a null divisor of $\{A_n\}$.

Next, suppose that p is a prime null divisor of $\{A_n\}$ such that $p \mid A_n$ for all $n \geq k$, where $k \geq 0$ is minimal. Since $A_1 = 1$, we cannot have $k = 0, 1$. If $k = 2$, then since $p \mid A_n$ $(n \geq 2)$ and

$$A_5 = P_1A_4 - (P_2 + 2Q)A_3 + P_1QA_2 - Q^2A_1$$

we see that $p \mid Q$ and $p \mid (A_2, A_3, Q)$. If $k \geq 3$, then $p \mid A_k$, $p \mid A_{k+1}$, $p \mid A_{k+2}$, $p \mid A_{k+3}$, but $p \nmid A_{k-1}$. Since

$$A_{k+3} = P_1 A_{k+2} - (P_2 + 2Q)A_{k+1} + P_1 Q A_k - Q^2 A_{k-1}$$

we see that $p \mid Q$. Also, since

$$A_{k+1} = P_1 A_k - (P_2 + 2Q)A_{k-1} + P_1 Q A_{k-2} - Q^2 A_{k-3}$$

we get $p \mid P_2 A_{k-1}$; hence $p \mid P_2$ and $p \mid (A_3, P_2, Q)$ when $k = 3$. If $k > 3$, then $A_k \equiv P_1 A_{k-1} \pmod{p}$ and $p \mid (P_1, P_2, Q)$. □

In the case of $\{U_n\}$ in [12], we have $U_2 = P_1$, $U_3 = P_1^2 - P_2 - 3Q$. Hence, since $(P_1, P_2, Q) = 1$, we see that $(U_3, P_2, Q) = 1$ and $(U_3, U_2, Q) = 1$. It follows that the single condition that $(P_1, P_2, Q) = 1$ ensures that $\{U_n\}$ has no null divisors.

In what follows, we shall investigate the possibility that a non null divisibility sequence $\{A_n\}$ could be neither even nor odd when both S and G are not 1. A very useful tool which we utilize heavily in this study is a paper of Hall [1]. We will modify Hall's argument to apply to our particular case of using $F(x)$ given by (2.2), but we will not repeat his arguments when there is no need and we simply refer the reader to [1] to fill in any gaps that we will leave in our presentation. In the sequel we will consider $\{A_n\}$ to be a non null divisibility sequence having characteristic polynomial given by (2.2) with nonzero discriminant.

Lemma 4.2. *Under the above conditions on $\{A_n\}$, suppose that a prime p is such that $p \mid Q$ and $p \mid A_n$ $(n > 0)$. Then there exists a finite N (independent of n and the choice of p) and a factor r of n such that $1 < r < N$.*

Proof. We use the same reasoning as Hall in his proof of his Lemma 1, together with Proposition 4.1. □

Lemma 4.3. *Let D be the discriminant of $F(x)$ (see (2.4)). If p is a prime divisor of A_n $(n > 0)$ and $p \mid D$, then there exists a finite N (independent of n and the choice of p) and a factor r of n such that $1 < r < N$.*

Proof. This follows exactly as the proof of Lemma 2 of [1]. □

Lemma 4.4. *Let N be defined as in Lemma 4.3 and q be a prime such that $q > N$, then $A_q^4 \equiv A_{q^2}^4 \equiv A_{q^3}^4 \equiv 1 \pmod{q}$.*

Proof. Let p be any prime divisor of A_q. Since $q > N$, we know that $p \nmid D$ by Lemma 4.3. If α_1, β_1, α_2, β_2 are the zeroes of $F(x)$ over the splitting field $\mathbb{K}$ of $F(x) \in \mathbb{F}_p[x]$, then

$$\alpha_1^{p^4-1} = \beta_1^{p^4-1} = \alpha_2^{p^4-1} = \beta_2^{p^4-1} = 1$$

in $\mathbb{K}$. It follows that for any $n \geq 0$, we have $A_{n+p^4-1} = A_n$ in $\mathbb{K}$. Since $\{A_n\} \subseteq \mathbb{Z}$, we must have $A_{n+p^4-1} \equiv A_n \pmod{p}$. The result now follows by using Hall's reasoning in the proof of his Lemma 3. □

In what follows we will attempt to determine the values of c_1, c_2, c_3, c_4 in (2.6) such that $\{A_n\}$ will be a divisibility sequence.

Lemma 4.5. *If there exists an infinitude of primes q such that $\left(\frac{\Delta}{q}\right) = \left(\frac{E}{q}\right) = -1$, then*

$$\begin{aligned} c_1\alpha_2 + c_2\beta_2 + c_3\beta_1 + c_4\alpha_1 &= \epsilon_1 \\ c_1\beta_1 + c_2\alpha_1 + c_3\beta_2 + c_4\alpha_2 &= \epsilon_2 \\ c_1\beta_2 + c_2\alpha_2 + c_3\alpha_1 + c_4\beta_1 &= \epsilon_3 \end{aligned}$$

where $\epsilon_1^4 = \epsilon_2^4 = \epsilon_3^4 = 1$.

Proof. If $\left(\frac{\Delta}{q}\right) = \left(\frac{E}{q}\right) = -1$, then $F(x)$ is irreducible modulo q and we have

$$\alpha_2 \equiv \alpha_1^q, \quad \beta_1 \equiv \alpha_1^{q^2}, \quad \beta_2 \equiv \alpha_1^{q^3}, \quad \alpha_1 \equiv \alpha_1^{q^4}, \qquad (\text{mod } \mathfrak{q})$$

where $\mathfrak{q}$ is a prime ideal lying over q in the maximal order of $\mathbb{Q}(\alpha_1, \alpha_2)$. It follows that

$$\begin{aligned} A_q &= c_1\alpha_1^q + c_2\beta_1^q + c_3\alpha_2^q + c_4\beta_2^q \\ &\equiv c_1\alpha_2 + c_2\beta_2 + c_3\beta_1 + c_4\alpha_1 \qquad (\text{mod } \mathfrak{q}). \end{aligned}$$

By Lemma 4.4 we get

$$(c_1\alpha_2 + c_2\beta_2 + c_3\beta_1 + c_4\alpha_1)^4 \equiv 1 \pmod{\mathfrak{q}}.$$

Since there exists an infinite number of possible primes q, we see that

$$(c_1\alpha_2 + c_2\beta_2 + c_3\beta_1 + c_4\alpha_1)^4 - 1$$

is divisible by an infinite number of distinct prime ideals, which can only mean that

$$(c_1\alpha_2 + c_2\beta_2 + c_3\beta_1 + c_4\alpha_1)^4 = 1$$

or

$$c_1\alpha_2 + c_2\beta_2 + c_3\beta_1 + c_4\alpha_1 = \epsilon_1$$

where $\epsilon_1^4 = 1$.

The other equations follow on employing similar reasoning on A_{q^2} and A_{q^3}. □

Lemma 4.6. *If there exists an infinitude of primes q such that $\left(\frac{\Delta}{q}\right) = 1$ and $\left(\frac{E}{q}\right) = -1$, then $c_1\alpha_1 + c_2\beta_1 + c_3\beta_2 + c_4\alpha_2 = \epsilon_4$, where $\epsilon_4^4 = 1$.*

Proof. If $\left(\frac{\Delta}{q}\right) = 1$ and $\left(\frac{E}{q}\right) = -1$, then without loss of generality we have

$$\alpha_1^q \equiv \alpha_1, \quad \beta_1^q \equiv \beta_1, \quad \alpha_2^q \equiv \beta_2, \quad \beta_2^q \equiv \alpha_2 \pmod{\mathfrak{q}}$$

where $\mathfrak{q}$ is a prime ideal lying over q in the maximal order of $\mathbb{Q}(\alpha_1, \alpha_2)$. The result can be derived by following the reasoning employed in the proof of Lemma 4.5. □

Lemma 4.7. *If* $d = (\alpha_1 - \beta_1)^2 + (\alpha_2 - \beta_2)^2 = 0$, *then* $4E = -\Delta P_1^2$.

Proof. We have $d = \rho_1^2 + \rho_2^2 - 8Q = P_1^2 - 2P_2 - 8Q$. The result now follows from (2.5). □

5. The Case of $S \neq 1$ and $G \neq 1$

We have seen in [13] that if $S \neq 1$ and $G \neq 1$, then there exists an infinitude of primes q such that $\left(\frac{\Delta}{q}\right) = \left(\frac{S}{q}\right) = -1$ and $\left(\frac{E}{q}\right) = \left(\frac{G}{q}\right) = -1$. We are now able to prove the following theorem.

Theorem 5.1. *If* $S \neq 1$, $G \neq 1$ *and* $S \neq -G$, *then* $\{A_n\}$ *must be either even or odd.*

Proof. Since $A_0 = 0$ and $A_1 = 1$, by Lemma 4.5 and (2.6) we have

$$c_1 + c_2 + c_3 + c_4 = 0 \tag{5.1}$$
$$c_1\alpha_1 + c_2\beta_1 + c_3\alpha_2 + c_4\beta_2 = 1 \tag{5.2}$$
$$c_1\alpha_2 + c_2\beta_2 + c_3\beta_1 + c_4\alpha_1 = \epsilon_1 \tag{5.3}$$
$$c_1\beta_1 + c_2\alpha_1 + c_3\beta_2 + c_4\alpha_2 = \epsilon_2 \tag{5.4}$$
$$c_1\beta_2 + c_2\alpha_2 + c_3\alpha_1 + c_4\beta_1 = \epsilon_3 \tag{5.5}$$

where $\epsilon_1^4 = \epsilon_2^4 = \epsilon_3^4 = -1$. If we add equations (5.2), (5.3), (5.4) and (5.5), we get

$$(c_1 + c_2 + c_3 + c_4)(\alpha_1 + \beta_1 + \alpha_2 + \beta_2) = 1 + \epsilon_1 + \epsilon_2 + \epsilon_3$$

and from (5.1), this means that

$$1 + \epsilon_1 + \epsilon_2 + \epsilon_3 = 0. \tag{5.6}$$

If we add (5.2) and (5.4) we get

$$(c_1 + c_2)(\alpha_1 + \beta_1) + (c_3 + c_4)(\alpha_2 + \beta_2) = 1 + \epsilon_2.$$

If we put $\delta = \alpha_1 + \beta_1 - \alpha_2 - \beta_2 = \rho_1 - \rho_2\,(\neq 0)$, then, by (5.1), we find that

$$c_1 + c_2 = (1 + \epsilon_2)/\delta,\ c_3 + c_4 = -(1 + \epsilon_2)/\delta. \tag{5.7}$$

If $\epsilon_2 = -1$, then $c_1 = -c_2$, $c_3 = -c_4$ and $\{A_n\}$ must be odd by Theorem 2.2.

Set $\lambda_i = \alpha_i - \beta_i$ $(i = 1, 2)$. On subtracting (5.4) from (5.2) we get

$$(c_1 - c_2)\lambda_1 + (c_3 - c_4)\lambda_2 = 1 - \epsilon_2$$

and on subtracting (5.5) from (5.3) we also get

$$(c_1 - c_2)\lambda_2 - (c_3 - c_4)\lambda_1 = \epsilon_1 - \epsilon_3.$$

On solving these two equations for $c_1 - c_2$ and $c_3 - c_4$, we find that

$$(c_1 - c_2)d = (\epsilon_1 - \epsilon_3)\lambda_2 + (1 - \epsilon_2)\lambda_1, \tag{5.8}$$
$$(c_3 - c_4)d = -(\epsilon_1 - \epsilon_3)\lambda_1 + (1 - \epsilon_2)\lambda_2. \tag{5.9}$$

Since $S \neq -G$, by Lemma 4.7 we cannot have $d = 0$.

If $\epsilon_2 = 1$, then by (5.6), $\epsilon_1 + \epsilon_3 = -2$. Since $\epsilon_1, \epsilon_3 \in \{1, -1, i, -i\}$, where $i^2 + 1 = 0$, we can only have $\epsilon_1 = \epsilon_3 = -1$. By (5.8) and (5.9) this means that $c_1 = c_2$, $c_3 = c_4$ and $\{A_n\}$ must be even by Theorem 2.2.

We next consider the case of $\epsilon_2^2 = -1$. By (5.6) we can only have $\epsilon_1 = -1$, $\epsilon_3 = -\epsilon_2$ or $\epsilon_3 = -1$, $\epsilon_1 = -\epsilon_2$. Hence $\epsilon_1 - \epsilon_3 = \eta(1 - \epsilon_2)$, where $\eta \in \{1, -1\}$. From (5.7), (5.8) and (5.9) we get

$$\begin{aligned}
2c_1 &= (1 - \epsilon_2)(\eta\lambda_2 + \lambda_1)/d + (1 + \epsilon_2)/\delta, \\
2c_2 &= (1 - \epsilon_2)(-\eta\lambda_2 - \lambda_1)/d + (1 + \epsilon_2)/\delta, \\
2c_3 &= (1 - \epsilon_2)(-\eta\lambda_1 + \lambda_2)/d - (1 + \epsilon_2)/\delta, \\
2c_4 &= (1 - \epsilon_2)(\eta\lambda_1 - \lambda_2)/d - (1 + \epsilon_2)/\delta.
\end{aligned}$$

On substituting these values of c_1, c_2, c_3, c_4 into (2.6) we get

$$2A_n = (1 - \epsilon_2)\left([\lambda_1^2 + \lambda_2^2]X_n + [\rho_1\lambda_1^2 + \rho_2\lambda_2^2 + \eta\lambda_1\lambda_2(\rho_1 - \rho_2)]Y_n\right)/d + (1 + \epsilon_2)U_n.$$

Put $C = \rho_1\lambda_1^2 + \rho_2\lambda_2^2 = P_1(P_1^2 - 3P_2 - 4Q) \in \mathbb{Z}$. Since $\lambda_1^2\lambda_2^2(\rho_1 - \rho_2)^2 = \Delta E$, we have $\eta\lambda_1\lambda_2(\rho_1 - \rho_2) = \pm\sqrt{\Delta E}$.

Since A_2 must be an integer and

$$2A_2 = (1 - \epsilon_2)(C \pm \sqrt{\Delta E})/d + (1 - \epsilon_2)P_1$$

we get

$$2dA_2 - dP_1 - C = \pm\sqrt{\Delta E} - \epsilon_2 C - \epsilon_2(\pm\sqrt{\Delta E}).$$

If we put $M = 2dA_2 - dP_1 - C \in \mathbb{Z}$, then

$$M \pm \sqrt{\Delta E} = -\epsilon_2(C \pm \sqrt{\Delta E} - P_1 d).$$

Squaring both sides, we find that, since $\epsilon_2^2 = -1$,

$$M^2 + (C - P_1 d)^2 + 2\Delta E = \mp 2(C - P_1 d - M)\sqrt{\Delta E}.$$

If $G \neq S$, then ΔE is not a square and $\sqrt{\Delta E} \notin \mathbb{Q}$. Hence $M = C - P_1 d$ and $2M^2 + 2\Delta E = 0$. But if $M^2 + \Delta E = 0$, then $G = -S$, which is not possible; hence, we must have $G = S$. In this case $R = [C + \eta\lambda_1\lambda_2(\rho_1 - \rho_2)]/d \in \mathbb{Q}$ and

$$2A_n = X_n + U_n + RY_n + \epsilon_2(U_n - X_n - RY_n).$$

Since $\epsilon_2(U_n - X_n - RY_n) \notin \mathbb{Q}$, we must have

$$U_n = X_n + RY_n.$$

Putting $n = 2$, we see that R must be P_1. Putting $n = 3$, we must have

$$U_3 = P_1^2 - P_2 - 3Q = X_3 + P_1 Y_3 = -Q - P_2 + P_1^2$$

which means that $Q = 0$, a contradiction. Hence $\epsilon_2^2 \neq -1$ and we have proved Theorem 5.1. □

Theorem 5.2. *Under the conditions of Theorem 5.1, we cannot have $\{A_n\}$ odd unless $S = G$.*

Proof. We have already seen in the proof of Theorem 5.1 that $\{A_n\}$ can be odd only when $\epsilon_2 = -1$. From (5.2) and (5.3) we get

$$\begin{aligned} c_1\lambda_1 + c_3\lambda_2 &= 1, \\ c_1\lambda_2 - c_3\lambda_1 &= \epsilon_1. \end{aligned}$$

It follows that $c_1 = (\lambda_1 + \epsilon_1\lambda_2)/d$, $c_3 = (\lambda_2 - \lambda_1\epsilon_1)/d$, and since $c_1 = -c_2$, $c_3 = -c_4$ when $\epsilon_2 = -1$, we get $dA_2 = \rho_1\lambda_1^2 + \rho_2\lambda_2^2 + (\rho_1 - \rho_2)\lambda_1\lambda_2\epsilon_1 = C \pm \epsilon_1\sqrt{\Delta E}$ from (2.6). Since $dA_2 - C \in \mathbb{Z}$, we must have $\sqrt{\Delta E} \in \mathbb{Z}$, which means that $S = G$. □

We next deal with the case where $G = -S$ and $S \neq 1$, $G \neq 1$. Here we still have equations (5.1), (5.2), (5.3), (5.4) and (5.5) and by Lemma 4.6 the additional equation

$$c_1\alpha_1 + c_2\beta_1 + c_3\beta_2 + c_4\alpha_2 = \epsilon_4 \tag{5.10}$$

where $\epsilon_4^4 = 1$.

Theorem 5.3. *If $S \neq 1$ and $G \neq 1$ and $G = -S$, then $\{A_n\}$ is either even or odd.*

Proof. If we subtract (5.10) from (5.2) we get

$$c_3\lambda_2 - c_4\lambda_2 = 1 - \epsilon_4.$$

Thus, from (5.7) we deduce

$$\begin{aligned} 2c_3 &= (1 - \epsilon_4)/\lambda_2 - (1 + \epsilon_2)/\delta, \\ 2c_4 &= (\epsilon_4 - 1)/\lambda_2 - (1 + \epsilon_2)/\delta. \end{aligned}$$

Also, since $c_1\alpha_1 + c_2\beta_1 = 1 - c_3\alpha_2 - c_4\beta_2 = (1 + \epsilon_4)/2 + (1 + \epsilon_2)\rho_2/2\delta$, we get

$$\begin{aligned} 2c_1 &= (\epsilon_4 - \epsilon_2)/\lambda_1 + (1 + \epsilon_2)/\delta, \\ 2c_2 &= (\epsilon_2 - \epsilon_4)/\lambda_1 + (1 + \epsilon_2)/\delta. \end{aligned}$$

Hence

$$2A_2 = (1 + \epsilon_2)(\alpha_1^2 + \beta_1^2 - \alpha_2^2 - \beta_2^2)/\delta - (\epsilon_2 - \epsilon_4)\rho_1 + (1 - \epsilon_4)\rho_2$$

or

$$2A_2 = (1 + \epsilon_2)P_1 - (1 - \epsilon_4)\delta + (1 - \epsilon_2)\rho_1.$$

We have already shown in the proof of Theorem 5.1 that if $\epsilon_2 = -1$, then $\{A_n\}$ must be odd. Suppose $\epsilon_2 = 1$. In this case

$$2(A_2 - P_1) = (\epsilon_4 - 1)\delta.$$

If we square both sides, we get

$$(\epsilon_4^2 + 1 - 2\epsilon_4)\Delta = 4(A_2 - P_1)^2.$$

If $\epsilon_4^2 = -1$, then $\epsilon_4\Delta \in \mathbb{Q}$, which is impossible. Thus, $\epsilon_4^2 = 1$. If $\epsilon_4 = 1$, then $\epsilon_4 = \epsilon_2 = 1$ and $c_1 = c_2$, $c_3 = c_4$; hence $\{A_n\}$ is even. If $\epsilon_4 = -1$, then $A_2 = P_1 - \delta$ and therefore Δ is a square. However, this means that $S = 1$, which is not possible. Thus, if $\{A_n\}$ is neither even nor odd, we must have $\epsilon_2^2 = -1$.

Suppose $\epsilon_2^2 = -1$ and $\epsilon_4 = 1$. In this case we get

$$2A_2 = (1 + \epsilon_2)P_1 + (1 - \epsilon_2)\rho_1$$

and

$$2A_2 - P_1 = \epsilon_2\rho_2 + \rho_1 \qquad (P_1 = \rho_1 + \rho_2).$$

Thus $(\epsilon_2\rho_2 + \rho_1)^2 = P_1(\rho_1 - \rho_2) + 2\epsilon_2 P_2 \in \mathbb{Z}$; consequently,

$$(P_1(\rho_1 - \rho_2) + 2\epsilon_2 P_2)^2 = P_1^2\Delta + 4\epsilon_2 P_2 P_1(\rho_1 - \rho_2) - 4P_2^2 \in \mathbb{Z}$$

and

$$4\epsilon_2 P_1 P_2(\rho_1 - \rho_2) \in \mathbb{Z}.$$

It follows that $-16P_1^2P_2^2\Delta$ is a square, but this means that $S = -1$ and $G = 1$, a contradiction.

If $\epsilon_4 = -1$, then

$$2A_2 = (1 + \epsilon_2)P_1 - 2\delta + (1 - \epsilon_2)\rho_1 = \rho_2(3 + \epsilon_2).$$

Since $3 + \epsilon_2 \neq 0$, we get $\rho_2 = 2A_2/(3 + \epsilon_2)$. We also recall that $\rho_2^2 - P_1\rho_2 + P_2 = 0$; hence by substitution of this value of P_2 we get

$$4A_2^2 - 6P_1A_2 + 8P_2 + (6P_2 - 2P_1A_2)\epsilon_2 = 0.$$

Since $\epsilon_2 \notin \mathbb{Q}$, we must have $A_2 = 3P_2/P_1$ $(P_1 \neq 0)$ and $4A_2^2 - 6P_1A_2 + 8P_2 = 0$, which means that $36P_2^2 = 10P_1^2P_2$.

If $P_2 = 0$, then $\Delta = P_1^2$, which is not possible. Hence $P_2 = 5P_1^2/18$ and $\Delta = -P_1^2/9$, which means that $S = -1$ and $G = 1$, an impossibility.

Thus, if $\epsilon_2^2 = -1$, we must have $\epsilon_4^2 = -1$ and $\epsilon_4 = \pm\epsilon_2$. If $\epsilon_4 = \epsilon_2$, then

$$2A_2 = (1 + \epsilon_2)P_1 - (1 - \epsilon_2)\delta + (1 - \epsilon_2)\rho_1$$

and

$$2A_2 - P_1 = \epsilon_2\rho_1 + \rho_2.$$

If $\epsilon_4 = -\epsilon_2$, then

$$2A_2 = (1+\epsilon_2)P_1 - (1+\epsilon_2)\delta + (1-\epsilon_2)\rho_1$$

and

$$2A_2 - P_1 = \epsilon_2(2\rho_2 - \rho_1) + \rho_2.$$

By using the same kind of reasoning as that employed above, we find that, since $S \neq 1$, $G \neq 1$ and $S = -G$, neither of these cases can occur. □

Theorem 5.4. *Under the conditions of Theorem 5.3 we cannot have $\{A_n\}$ odd.*

Proof. From the proof of Theorem 5.3 we have

$$2A_2 = (1+\epsilon_2)P_1 - (1-\epsilon_4)\delta + (1-\epsilon_2)\rho_1.$$

We know from the proof of Theorem 5.1 that $\{A_n\}$ can be odd only when $\epsilon_2 = -1$. Under this condition

$$2A_2 = P_1 + \epsilon_4\delta$$

and if $\epsilon_4^4 = 1$, then $(2A_2 - P_1)^2 = \pm\Delta$ which implies that $S = 1$ or $S = -1$ and $G = 1$, both of which are excluded by the conditions of Theorem 5.3. □

6. Some Cases When S or G is 1

We have seen that if $S \neq 1$ and $G \neq 1$, the only divisibility sequences $\{A_n\}$ must be either even or odd. We now briefly consider the cases where $S = 1$ or $G = 1$.

If $S = 1$ and $G \neq 1$, we have $\Delta = V^2$ $(V \in \mathbb{Z})$, $\rho_1 = (P_1 + V)/2 \in \mathbb{Z}$, $\rho_2 = (P_1 - V)/2 \in \mathbb{Z}$. Put $R_i = \rho_i^2 - 4Q$ $(i = 1, 2)$. Then $E = R_1R_2$. Since R_1R_2 is not a square, if neither R_1 nor R_2 is a square, there must exist infinite sets of primes q such that either

$$\left(\frac{R_1}{q}\right) = \left(\frac{R_2}{q}\right) = -1; \text{ or } \left(\frac{R_1}{q}\right) = -1, \left(\frac{R_2}{q}\right) = 1; \text{ or } \left(\frac{R_1}{q}\right) = 1, \left(\frac{R_2}{q}\right) = -1.$$

Also, if p is a prime and $\left(\frac{R_i}{p}\right) = -1$ $(i = 1, 2)$, then in the maximal order of $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\sqrt{R_1}, \sqrt{R_2})$, we have

$$\alpha_i^p \equiv \beta_i \pmod{p}, \quad \beta_i^p \equiv \alpha_i \pmod{p} \quad (i = 1, 2)$$

and if $\left(\frac{R_i}{p}\right) = 1$ $(i = 1, 2)$, then

$$\alpha_i^p \equiv \alpha_i \pmod{p}, \quad \beta_i^p \equiv \beta_i \pmod{p} \quad (i = 1, 2).$$

By (2.6) we see that

$$A_{n+p^2-1} \equiv A_n \pmod{p}$$

for any prime p such that $p \nmid 2D$ for any $n \geq 0$. It follows that $A_q^2 \equiv 1 \pmod{q}$ if q is any prime such that $q > N$ (Lemma 4.3).

We also find that if $\{A_n\}$ is to be a divisibility sequence, we must have

$$\begin{aligned} c_1 + c_2 + c_3 + c_4 &= 0 \\ c_1\alpha_1 + c_2\beta_1 + c_3\alpha_2 + c_4\beta_2 &= 1 \\ c_1\alpha_1 + c_2\beta_1 + c_3\beta_2 + c_4\alpha_2 &= \epsilon_1 \\ c_1\beta_1 + c_2\alpha_1 + c_3\alpha_2 + c_4\beta_2 &= \epsilon_2 \\ c_1\beta_1 + c_2\alpha_1 + c_3\beta_2 + c_4\alpha_2 &= \epsilon_3 \end{aligned}$$

where $\epsilon_1^2 = \epsilon_2^2 = \epsilon_3^2 = 1$. We can then deduce that $1 + \epsilon_3 = \epsilon_1 + \epsilon_2$ and

$$2c_1 = (\epsilon_1 + \epsilon_2)/\delta - (\epsilon_2 - 1)/\lambda_1, \quad 2c_2 = (\epsilon_1 + \epsilon_2)/\delta + (\epsilon_2 - 1)/\lambda_1,$$

$$2c_3 = -(\epsilon_1 + \epsilon_2)/\delta - (\epsilon_1 - 1)/\lambda_2, \quad 2c_4 = -(\epsilon_1 + \epsilon_2)/\delta + (\epsilon_1 - 1)/\lambda_2.$$

Since $1 + \epsilon_3 = \epsilon_1 + \epsilon_2$, we can only have $\epsilon_1 = \epsilon_2 = 1$ or $\epsilon_1 = -\epsilon_2$. In the former case we get $c_1 = c_2$, $c_3 = c_4$ and $\{A_n\}$ must be even. In the latter case we get $c_1 = -c_2$, $c_3 = -c_4$ and $\{A_n\}$ must be odd.

Thus, if $G \neq 1$, $\Delta = V^2$, and neither of $P_1^2 \pm 2VP_1 + \Delta - 16Q$ is a square, then $\{A_n\}$ is either even or odd. We also note in this case that we have

$$c_1\alpha_1 + c_2\beta_1 + c_3\beta_2 + c_4\alpha_2 = \epsilon_1 \quad (\epsilon_1^2 = 1).$$

If $\{A_n\}$ is odd, then since $c_1 = -c_2$, $c_3 = -c_4$, we get

$$c_1\lambda_1 + c_3\lambda_2 = 1, \quad c_1\lambda_1 - c_3\lambda_2 = \epsilon_1.$$

Thus, $2c_1\lambda_1 = 1 + \epsilon_1$, $2c_3\lambda_2 = 1 - \epsilon_1$. It follows that either $c_1 = 0$ or $c_3 = 0$ and therefore A_n is one of the Lucas functions $u_n(\rho_i, Q)$ $(i = 1 \text{ or } 2)$.

We next consider the case where $S \neq 1$, $G = 1$ and $E = U^2$ where $U \in \mathbb{Z}$. We have seen in [13] that there must exist integers r_1, r_2, q_1, q_2 satisfying $r_i > 0$ and $(r_i, q_i) = 1$ for $i = 1, 2$, such that

$$P_1^2 = r_1 r_2, \quad P_2 = q_1 r_2 + q_2 r_1 - 4q_1 q_2, \quad Q = q_1 q_2, \quad U = q_1 r_2 - q_2 r_1.$$

Here we have $\alpha_1 = \mu_1\mu_2$, $\beta_1 = \nu_1\nu_2$, $\alpha_2 = \nu_1\mu_2$ and $\beta_2 = \mu_1\nu_2$, where $\mu_i + \nu_i = \sqrt{r_i}$, $\mu_i\nu_i = q_i$ $(i = 1, 2)$. Also, $\Delta = d_1 d_2$, where $d_i = r_i - 4q_i$ $(i = 1, 2)$.

In the maximal order of $\mathbb{Q}(\mu_1, \mu_2)$ we have, for any prime p such that $p \nmid 2D$,

$$\mu_i^p \equiv \begin{cases} \left(\frac{r_i}{p}\right)\mu_i \pmod{p} & \text{when } \left(\frac{d_i r_i}{p}\right) = 1 \\ \left(\frac{r_i}{p}\right)\nu_i \pmod{p} & \text{when } \left(\frac{d_i r_i}{q}\right) = -1. \end{cases}$$

Hence

$$\alpha_1^p \equiv \beta_2,\ \beta_1^p \equiv \alpha_2,\ \alpha_2^p \equiv \beta_1,\ \beta_2^p \equiv \alpha_1 \pmod p$$

when $\left(\frac{d_1r_1}{p}\right) = 1$, $\left(\frac{d_2r_2}{p}\right) = -1$. Also

$$\alpha_1^p \equiv \alpha_2,\ \beta_1^p \equiv \beta_2,\ \alpha_2^p \equiv \alpha_1,\ \beta_2^p \equiv \beta_1 \pmod p$$

when $\left(\frac{d_1r_1}{p}\right) = -1$, $\left(\frac{d_2r_2}{p}\right) = 1$ and

$$\alpha_1^p \equiv \beta_1,\ \beta_1^p \equiv \alpha_1,\ \alpha_2^p \equiv \beta_2,\ \beta_2^p \equiv \alpha_2 \pmod p$$

when $\left(\frac{d_1r_1}{p}\right) = -1$, $\left(\frac{d_2r_2}{p}\right) = -1$. In all possible cases, including $\left(\frac{d_1r_1}{p}\right) = \left(\frac{d_2r_2}{p}\right) = 1$, we find that

$$\alpha_i^{p^2} \equiv \alpha_i,\ \beta_i^{p^2} \equiv \beta_i \pmod p \quad \text{for } i = 1, 2.$$

Hence, $A_{p^2-1+n} \equiv A_n \pmod p$. It follows from Hall's reasoning that if neither d_1r_1 nor d_2r_2 is a perfect square, then we must have

$$\begin{aligned} c_1 + c_2 + c_3 + c_4 &= 0 \\ c_1\alpha_1 + c_2\beta_1 + c_3\alpha_2 + c_4\beta_2 &= 1 \\ c_1\beta_2 + c_2\alpha_2 + c_3\beta_1 + c_4\alpha_1 &= \epsilon_1 \\ c_1\alpha_2 + c_2\beta_2 + c_3\alpha_1 + c_4\beta_1 &= \epsilon_2 \\ c_1\beta_1 + c_2\alpha_1 + c_3\beta_2 + c_4\alpha_2 &= \epsilon_3 \end{aligned}$$

where $\epsilon_1^2 = \epsilon_2^2 = \epsilon_3^2 = 1$. By adding these equations we get

$$1 + \epsilon_1 + \epsilon_2 + \epsilon_3 = 0.$$

We can also deduce that

$$c_1 + c_2 = -(\epsilon_1 + \epsilon_2)/\delta, \qquad c_3 + c_4 = (\epsilon_1 + \epsilon_2)/\delta.$$

If $\epsilon_3 = -1$, then $\epsilon_1 + \epsilon_2 = 0$ and $c_1 = -c_2$, $c_3 = -c_4$, which means that $\{A_n\}$ is odd. If $\epsilon_3 = 1$, then $\epsilon_1 = \epsilon_2 = -1$ and

$$\begin{aligned} (c_1 - c_2)\lambda_1 + (c_3 - c_4)\lambda_2 &= 0, \\ (c_1 - c_2)\lambda_2 + (c_3 - c_4)\lambda_1 &= 0. \end{aligned}$$

Since $\lambda_1^2 - \lambda_2^2 = P_1\delta \neq 0$, we have $c_1 = c_2$ and $c_3 = c_4$ and $\{A_n\}$ is even.

Now $(P_2 + 4Q - U)/2 = q_2r_1$ and $(P_2 + 4Q + U)/2 = q_1r_2$; hence $r_1 = q_1(P_2 + 4Q - U)/2Q$, $r_2 = q_2(P_2 + 4Q + U)/2Q$. Hence $d_1 = q_1(P_2 - 4Q - U)/2Q$, $d_2 = q_2(P_2 - 4Q + U)/2Q$. and

$$4Q^2d_1r_1 = q_1^2[(P_2 - U)^2 - 16Q^2], \quad 4Q^2d_2r_2 = q_2^2[(P_2 + U)^2 - 16Q^2].$$

Thus, if $E = U^2$ and neither of $(P_2 \pm U)^2 - 16Q^2$ is a square, then $\{A_n\}$ is either even or odd.

If $G = 1$, $S \neq 1$, and $\{A_n\}$ is odd, then since $c_2 = -c_1$, $c_4 = -c_3$, we get

$$c_1\lambda_1 + c_3\lambda_2 = 1, \quad c_1\lambda_2 + c_3\lambda_1 = \epsilon$$

where $\epsilon^2 = 1$. It follows that

$$c_1 = 1/(\lambda_1 + \epsilon\lambda_2), \quad c_2 = \epsilon/(\lambda_1 + \epsilon\lambda_2)$$

and we get

$$\begin{aligned} A_n &= \frac{1}{\lambda_1 + \epsilon\lambda_2}\left(\alpha_1^n - \beta_1^n + \epsilon(\alpha_2^n - \beta_2^n)\right) \\ &= \frac{(\mu_1^n + \epsilon\nu_1^n)(\mu_2^n - \epsilon\nu_2^n)}{(\mu_1 + \epsilon\nu_1)(\mu_2 - \epsilon\nu_2)}. \end{aligned}$$

Without loss of generality we can put $\epsilon = 1$ and we find that

$$A_n = v_n(\sqrt{r_1}, q_1)u_n(\sqrt{r_2}, q_2)/\sqrt{r_1}.$$

If $\{A_n\}$ is to be a divisibility sequence, we need $A_n \mid A_{2n}$, but this can only happen if

$$A_{2n}/A_n = (\mu_1^n + \nu_1^n)(\mu_2^n + \nu_2^n) - 2\mu_1^n\nu_1^n(\mu_2^n + \nu_2^n)/(\mu_1^n + \nu_1^n) \in \mathbb{Z}.$$

Now since $(\mu_1^n + \nu_1^n)(\mu_2^n + \nu_2^n) \in \mathbb{Z}$, we must have $2q_1^n(\mu_2^n + \nu_2^n)/(\mu_1^n + \nu_1^n) \in \mathbb{Z}$; thus, if $n = 1$, then we need $2q_1\sqrt{r_2/r_1} \in \mathbb{Z}$. Since $(q_1, r_1) = 1$, this means that $2\sqrt{r_2/r_1} \in \mathbb{Z}$. If we put

$$t_n = \begin{cases} 2 & 2 \mid n, \\ 2\sqrt{r_2/r_1} & 2 \nmid n. \end{cases}$$

We see that $A_{2n}/A_n \in \mathbb{Z}$ if and only if

$$\bar{v}_n(r_1, q_1) \nmid q_1^n t_n \bar{v}_n(r_2, q_2).$$

Since $(\bar{v}_n(r_1, q_1), q_1) = (r_1, q_1) = 1$, we see that $\{A_n\}$ is a divisibility sequence if and only if

$$\bar{v}_n(r_1, q_1) \mid t_n\bar{v}_n(r_2, q_2) \quad \text{for all } n \geq 0. \tag{6.1}$$

It is easy to show that if p is a prime, $p \nmid 2q$, and $p \mid \bar{v}_n(r, q)$, then there exists a minimal $\rho\,(> 0)$ such that $p \mid \bar{v}_\rho(r, q)$ and if $p \mid \bar{v}_m(r, q)$, then $\rho \mid m$. Also $\rho = \omega/2$, where ω is the rank of apparition of p in $\{\bar{u}_n(r, q)\}$. If we now define $\eta_1 = \eta_1(p) = \left(\frac{d_1 r_1}{p}\right)$, $\eta_2 = \eta_2(p) = \left(\frac{d_2 r_2}{p}\right)$, and $\theta_1 = \theta_1(p) = \left(\frac{q_1 r_1}{p}\right)$, we know from results of Lehmer [2] that

$$p \mid \bar{v}_{(p-\eta_1)/2}(r_1, q_1)$$

when $\theta_1 = -1$. Note that $\eta_1\eta_2 = \left(\frac{d_1 d_2}{p}\right) = \left(\frac{\Delta}{p}\right)$ because $r_1 r_2$ is a square. If we suppose that $r_1 q_1$ is not a square, then because $(d_1, q_1) = (r_1, q_1) = 1$, there must exist (see [13]) an infinitude of primes $p\,(> t_n)$ such that $\theta_1(p) = -1$, $\eta_1(p)\eta_2(p) = -1$ and $p \nmid 2q_1q_2$. For such primes we see that for $n = (p - \eta_1)/2$ we must have $p \mid \bar{v}_n(r_2, q_2)$ by (6.1) if $\{A_n\}$ is to be a divisibility sequence. If ρ is the least value of m such that $p \mid \bar{v}_m(r_2, q_2)$, then $\rho \mid n$. Now Lehmer [2] showed that if ω is the rank of apparition of p in $\{u_m(r_2, q_2)\}$, then ω must divide $p - \eta_2$. This means that $\rho \mid (p - \eta_2)/2$, but since $p \mid \bar{v}_n(r_2, q_2)$, we must have $\rho \mid n$ or $\rho \mid (p - \eta_1)/2$. Since $\eta_1\eta_2 = -1$, this is impossible unless $\rho = 1$, but in this case $\bar{v}_\rho(r_2, q_2) = 1$, a contradiction.

Thus, if $\{A_n\}$ is to be an odd divisibility sequence when $G = 1$ and $S \neq 1$, we must have $r_1 q_1$ a perfect square. Since $(r_1, q_1) = 1$, this means that both r_1 and q_1 must be perfect squares. Also, since $r_1 r_2$ is a square, we must have r_2 a perfect square. We note that $\bar{v}_n(s^2, q) = v_n(s, q)$ when $2 \mid n$ and $\bar{v}_n(s^2, q) = v_n(s, q)/s$ when $2 \nmid n$. Thus, if we put $r_1 = s_1^2$, $r_2 = s_2^2$, then, by (6.1), we must have

$$2v_n(s_2, q_2)/v_n(s_1, q_1) \in \mathbb{Z} \quad \text{for all } n \geq 0. \tag{6.2}$$

If $S \neq 1$, this seems most unlikely.

7. Conclusion

We now summarize some of our results. We let $\{A_n\}$ be any non null linear divisibility sequence with characteristic polynomial $F(x)$, given by (2.2) with nonzero discriminant and $P_1 \neq 0$. We let S, G be defined by (3.2).

1. If $S \neq 1$ and $G \neq 1$, $\{A_n\}$ can only be even or odd.
2. There is always one and only one even $\{A_n\}$ for any given $F(x)$.
3. If $S \neq 1$ and $G \neq 1$ and $G \neq S$, there can be no odd $\{A_n\}$.
4. If $S = 1$ and $G \neq 1$, then the only possible odd $\{A_n\}$ is the Lucas sequence $\{u_n\}$.

This leaves us with several unanswered questions.

1. If $G = 1$ or $S = 1$, what are the conditions on P_1, P_2, Q for the existence of an $\{A_n\}$ that is neither even nor odd? We have seen that if $P_1 = 0$ $(G = 1, S = 1)$, such a sequence does exist, but are there any when $P_1 \neq 0$?
2. Do any odd sequences $\{A_n\}$ exist when $S = G \neq 1$? No non-trivial example of such a sequence is known. We do have the case of $|P_1| = 1$, $P_2 = -1$, $Q = 1$, $|A_2| = 1$. In this case $\Delta = E = 5$, but $\{A_n\}$ is periodic with period 10 and $|A_n| = 1$ for all $n \in \mathbb{Z}$.

3. Do any odd divisibility sequences exist when $G = 1$ and $S \neq 1$? If so, then (6.2) must hold, and this seems very unlikely when $S \neq 1$.

4. What odd $\{A_n\}$ exist when $S = G = 1$?

In Section 2 we mentioned some odd divisibility sequences, and $S = G = 1$ for all of these. In fact, Oosterhout [4, §3.5.1] discovered an infinitude of odd $\{A_n\}$, where, if R and W are integer parameters and $R \mid W^2$, we put $P_1 = W^2/R - 3W$, $P_2 = W^3/R - 6W^2 + 10WR - 4R^2$, $Q = R^2$, $A_{-1} = -R^2$, $A_0 = 0$, $A_1 = 1$, $A_2 = W^2/R - 2W$. Here $\Delta = (W^2/R - 5W + 4R)^2$, $E = (W^3/R - 6W^2 + 8RW)^2$.

After making some minor corrections, we get these sequences from hers by replacing her Q by W and her Q^2/P by R. Also, if $\{A_n\}$ is to be non null, we must have $(R, W^2/R) = 1$ and $|R|$ a perfect square.

If we put $R = 1$, $W = 5$, we get $P_1 = 10$, $P_2 = 21$, $Q = 1$, $A_2 = 15$. This is A127595 in [7]; however, A215466 cannot be represented by any of Oosterhout's schemes. Thus it appears that there are more odd $\{A_n\}$ yet to be discovered, but it seems that such sequences will have $S = G = 1$.

Acknowledgements. The authors are grateful to Christian Ballot for drawing their attention to an example of a sequence $\{A_n\}$ that is neither even nor odd when $P_1 = 0$. They would also like to thank the meticulous and well-informed referee who enabled them to remove several obscurities and minor errors.

References

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

[2] D. H. Lehmer, An extended theory of Lucas functions, *Annals of Math.* **31**(1930) 419–448.

[3] E. Lucas, Théorie des fonctions numériques simplement périodiques *Amer. J. Math.*, **1** (1878) 184–240, 289–321.

[4] A. Oosterhout, *Characterisation of Divisibility Sequences*, Master's thesis. Utrecht Univ., 2011.

[5] G. Pólya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. reine angew. Math.* **151** (1920) 1–31.

[6] E. Roettger, H. C. Williams & R. K. Guy, Some extensions of the Lucas functions, in *Number Theory and related fields*, Springer, 2013, Chapter 15, 279–319.

[7] Neil Sloane, Online Encyclopedia of Integer Sequences, `http://oeis.org/wiki/`

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

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

[10] M. Ward, Prime divisors of second order recurring sequences, *Duke Math. J.* **21** (1954) 607–614.

[11] Hugh Cowie Williams, *Édouard Lucas and Primality Testing*. Canadian Mathematical Society Series of Monographs and Advanced Texts, **22**. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998.

[12] H. Williams & R. Guy, Some fourth order linear divisibility sequences, *Internat. J. Number Theory* **7** (2011) 1255-1277.

[13] H. Williams & R. Guy, Some monoapparitic fourth order divisibility sequences, *Integers* **12A** (2012) #17.