Journal of Integer Sequences, Vol. 24 (2021),
Article 21.7.5

Appearance of Primes in Fourth-Order Odd Divisibility Sequences

E. L. Roettger
Department of General Education
Mount Royal University
4825 Mount Royal Gate SW
Calgary, AB T3E 6K6
Canada
eroettger@mtroyal.ca

H. C. Williams
Department of Mathematics and Statistics
University of Calgary
2500 University Drive NW
Calgary, AB T2N 1N4
Canada
hwilliam@ucalgary.ca

Abstract

Let (A_n) denote any odd, non-degenerate, non-null, fourth-order linear divisibility sequence and let p be any prime such that p divides some term A_n $(n > 1)$ of (A_n). In this paper we derive a number of properties of (A_n). In particular, we exhibit conditions which guarantee that if $p \mid A_k$, then $\omega \mid k$. Here ω $(= \omega(p))$ is the least positive integer m such that $p \mid A_m$.

Dedicated to the memory of Richard Guy (1916–2020).

1 Introduction

Although we use the notation (T_n) to denote the sequence

$$\ldots, T_{-n}, \ldots, T_{-2}, T_{-1}, T_0, T_1, T_2, \ldots, T_n, \ldots,$$

we will often be concerned in the sequel with terms of (T_n) which have only positive subscripts. Let $p,\ q \in \mathbb{C}$ and $\alpha,\ \beta$ be the zeros of $x^2 - px + q \in \mathbb{C}[x]$. We define, for any $n \in \mathbb{Z}$,

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

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 integers are called the Lucas functions. Note that $u_0 = 0,\ u_1 = 1,\ v_0 = 2,\ v_1 = p$. The Lucas sequences $(u_n(p,q))$, $(v_n(p,q))$ both satisfy the second-order linear recurrence

$$T_{n+1} = pT_n - qT_{n-1}.$$

Also, $m \mid n \Rightarrow u_m(p,q) \mid u_n(p,q)$.

Definition 1. A *linear recurrence sequence of order* l over the integers is a sequence (T_n), where we have

$$T_{n+l} = A_1T_{n+l-1} + A_2T_{n+l-2} + A_3T_{n+l-3} + \ldots + A_lT_n$$

and $T_0,\ T_1,\ T_2,\ \ldots\ ,\ T_{l-1},\ A_1,\ A_2,\ A_3,\ \ldots\ ,\ A_l$ are given fixed integers, with $A_l \neq 0$. Furthermore, if $T_m \mid T_n$ whenever $m \mid n$, then (T_n) is said to be a l^{th} *order linear divisibility sequence* (LDS).

Thus, we see that the Lucas sequence $(u_n(p,q))$ is a second-order LDS.

In his investigation of the problem of primality testing, Lehmer [4] introduced the functions $(\bar{u}_n(r,q))$, $(\bar{v}_n(r,q))$, where $r,\ q$ are coprime integers. These are defined by

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

$$\bar{v}_n(r,q) = \begin{cases} v_n(\sqrt{r},q), & \text{if } 2 \mid n; \\ \dfrac{v_n(\sqrt{r},q)}{\sqrt{r}}, & \text{if } 2 \nmid n. \end{cases}$$

Notice that for n positive or negative

$$\bar{u}_{-n}(r,q) = -q^n\bar{u}_n(r,q), \quad \bar{v}_{-n}(r,q) = q^n\bar{v}_n(r,q).$$

The sequences $(\bar{u}_n(r,q))$, $(\bar{v}_n(r,q))$ are comprised of integers for all $n \geq 0$ and both satisfy the fourth-order linear recurrence

$$T_{n+4} = (r - 2q)T_{n+2} - q^2T_n. \tag{1}$$

Here we have $\bar{u}_0 = 0$, $\bar{u}_1 = 1$, $\bar{u}_2 = 1$, $\bar{u}_3 = r - q$, $\bar{v}_0 = 2$, $\bar{v}_1 = 1$, $\bar{v}_2 = r - 2q$, $\bar{v}_3 = r - 3q$. Furthermore, $(\bar{u}_n(r, q))$, is a divisibility sequence; hence $(\bar{u}_n(r, q))$ is a fourth-order LDS. We also know from results in [4] that $\bar{u}_{2n}(r, q) = \bar{u}_n(r, q)\bar{v}_n(r, q)$ and that $\bar{v}_n(r, q) \mid \bar{v}_{kn}(r, q)$ when k is odd.

Recently, by making use of the theory of generalized Vandermonde determinants, Barbero [2] was able to give an elementary proof of an important result of Bézivin, Pethö, and van der Poorten [3] in the specific case where the *characteristic polynomial* $F(x)$ $(= x^l - A_1x^{l-1} - A_2x^{l-2} - \ldots - A_l)$ of (T_n) has a non-zero discriminant, but his overall result is much more general than this.

Definition 2. We say that the sequence (T_n) is *degenerate* if α_i/α_j is a root of unity for any two distinct roots α_i, α_j of the characteristic polynomial $F(x)$.

Theorem 3. *If (T_n) is a non-degenerate LDS of order l whose characteristic polynomial has distinct roots $\alpha_1, \ldots, \alpha_l$, then, for all $n \geq 0$, we must have $T_n \mid r_n$, where*

$$r_n = \prod(\alpha_i^n - \alpha_j^n)/(\alpha_i - \alpha_j)$$

and the product is taken over all i and j such that $1 \leq i < j \leq l$.

Theorem 3 was used by Abrate et al. [1] to prove the following result.

Theorem 4. *If (T_n) is a non-degenerate LDS of order 4, then its characteristic polynomial must be the form*

$$x^4 - Px^3 + (R + 2Q)x^2 - PQx + Q^2,$$

for some integers P, Q and R.

The above polynomial is the characteristic polynomial for the Lehmer functions for $P = 0$, $Q = q$, $R = -r$.

Definition 5. If (T_n) is a linear recurrence sequence, we say that an integer m $(m > 1)$ is a *null divisor* of (T_n) if, for some minimal $h > 0$, we have $m \mid T_n$ for all $n \geq h$.

Definition 6. If (T_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 $\gcd(p, q) = 1$ ensures that both $(u_n(p, q))$ and $(v_n(p, q))$ are non-null sequences. Similarly, the condition that $\gcd(r, q) = 1$ ensures that both $(\bar{u}_n(r, q))$ and $(\bar{v}_n(r, q))$ are non-null sequences. Also, our attention will be confined to fourth-order sequences (T_n) which are both non-degenerate and non-null. Furthermore, as was done in Williams and Guy [12], we will only consider the case of $l = 4$ and (T_n) a divisibility sequence. By Theorem 4, we need only consider

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

where P_1, P_2 and Q are fixed integers, i.e.,

$$T_{n+4} = P_1 T_{n+3} - (P_2 + 2Q)T_{n+2} + P_1 Q T_{n+1} - Q^2 T_n. \tag{3}$$

Note that if D ($\neq 0$) is the discriminant of $F(x)$, then

$$D = E\Delta^2 Q^2, \tag{4}$$

where

$$\Delta = P_1^2 - 4P_2, \quad E = (P_2 + 4Q)^2 - 4QP_1^2. \tag{5}$$

See, for example, Williams and Guy [10]. Let ρ_1, ρ_2 be the roots of the quadratic polynomial $x^2 - P_1 x + P_2 = 0$. Since

$$F(x) = f_1(x) f_2(x),$$

where $f_i(x) = x^2 - \rho_i x + Q$, we may assume that if α_1, β_1, α_2, β_2 denote the four distinct roots of $F(x)$, then

$$\alpha_1 \beta_1 = \alpha_2 \beta_2 = Q. \tag{6}$$

Definition 7. We say that if (T_n) satisfies (3), then (T_n) is *even* when $T_{-n} = T_n/Q^n$ and (T_n) is *odd* when $T_{-n} = -T_n/Q^n$ for all n.

Certainly, if (T_n) is odd, we must have $T_0 = -T_0/Q^0 \Rightarrow T_0 = 0$ and $QT_{-1} = -T_1$. We now show that these two conditions are necessary and sufficient for (T_n) to be odd.

Theorem 8. *If $T_0 = 0$, then (T_n) is odd if and only if $QT_{-1} = -T_1$.*

Proof. If (T_n) is odd, then $QT_{-1} = -T_1$ from the definition. Suppose that $QT_{-1} = -T_1$. By (3) we have

$$\begin{aligned} T_2 &= P_1 T_1 - (P_2 + 2Q)T_0 + P_1 Q T_{-1} - Q^2 T_{-2} \\ &= P_1 T_1 - 0 - P_1 T_1 - Q^2 T_{-2} = -Q^2 T_{-2}. \end{aligned}$$

Also,

$$T_3 = P_1 T_2 - (P_2 + 2Q)T_1 + P_1 Q T_0 - Q^2 T_{-1} = P_1 T_2 - (P_2 + Q)T_1$$

and since

$$T_1 = P_1 T_0 - (P_2 + 2Q)T_{-1} + P_1 Q T_{-2} - Q^2 T_{-3},$$

we see that

$$\begin{aligned} -Q^3 T_{-3} &= QT_1 - (P_2 + 2Q)T_1 + P_1 T_2 \\ &= P_1 T_2 - (P_2 + 2Q)T_1 - Q^2 T_{-1} = T_3. \end{aligned}$$

Thus, $T_i = -Q^i T_{-i}$ $(i = 0, 1, 2, 3)$. If we assume that for some $m \geq 0$ we have $T_{m+i} = -Q^{m+i} T_{-(m+i)}$ $(i = 0, 1, 2, 3)$ (this is certainly true for $m = 0$), we can see that $T_m = -Q^m T_{-m}$, $T_{m+1+i} = -Q^{m+1+i} T_{-(m+1+i)}$ $(i = 0, 1, 2)$. We can now use (3) to compute

$$T_{m+1+3} = -Q^{m+2}(P_1 Q T_{-(m+3)} - (P_2 + 2Q)T_{-(m+2)} + P_1 T_{-(m+1)} - T_{-m}).$$

Also, by (3), we have

$$T_{-m} = P_1 T_{-(m+1)} - (P_2 + 2Q)T_{-(m+2)} + P_1 Q T_{-(m+3)} - Q^2 T_{-(m+4)}.$$

Putting this value of T_{-m} into the previous result, we get

$$T_{m+1+3} = T_{m+4} = -Q^{m+4} T_{-(m+4)} = -Q^{m+1+3} T_{-(m+1+3)}.$$

Thus, we find by induction that $T_n = -Q^n T_{-n}$ for all $n \geq 0$. □

If $T_0 = P_1 = 0$ and $T_1 = QT_{-1}$, we can show by using the above reasoning that

$$Q^n T_{-n} = (-1)^{n-1} T_n.$$

Thus, in this case we see that T_n is neither even nor odd.

We also have the following simple result, which extends an observation in [11, §1].

Proposition 9. *Suppose (T_n) satisfies (3). Let $\eta \in \{1, -1\}$ and suppose $T_j^* = \eta^{j-1} T_j$ $(j = -1, 0, 1, 2)$. If $P_1^* = \eta P_1$ and*

$$T_{n+4}^* = P_1^* T_{n+3}^* - (P_2 + 2Q)T_{n+2}^* + P_1^* Q T_{n+1}^* - Q^2 T_n^*,$$

then $T_n^* = \eta^{n-1} T_n$ for all $n \geq 1$.

Proof. Follows easily by induction on n. □

Suppose that $P_1 = 0$. If (T_n) satisfies (3), we have

$$T_{n+4} = -(P_2 + 2Q)T_{n+2} - Q^2 T_n. \tag{7}$$

If (T_n) is to be a non-degenerate LDS, we must have

$$1 + QT_{-1} = 0 \quad \text{or} \quad 1 - QT_{-1} = 0$$

by results in [12, §3]. In the case of $QT_{-1} = -1$, then

$$T_n = \begin{cases} T_2 \bar{u}_n(-P_2, Q), & \text{if } 2 \mid n; \\ \bar{u}_n(-P_2, Q), & \text{if } 2 \nmid n; \end{cases}$$

if $QT_{-1} = 1$, then

$$T_n = \begin{cases} T_2 \bar{u}_n(-P_2, Q), & \text{if } 2 \mid n; \\ \bar{v}_n(-P_2, Q), & \text{if } 2 \nmid n. \end{cases}$$

Note that in either event (T_n) is a divisibility sequence because $(\bar{u}_n(-P_2, Q))$ is a divisibility sequence, $\bar{v}_n(-P_2, Q) \mid \bar{v}_{nk}(-P_2, Q)$ when k is odd and $\bar{u}_{2n}(-P_2, Q) = \bar{u}_n(-P_2, Q)\bar{v}_n(-P_2, Q)$.

Now if we define $u_n^* = \bar{u}_n(-P_2 - 4Q, -Q)$, we see that since $-P_2 - 4Q + 2Q = -P_2 - 2Q$, then (u_n^*) must satisfy (7). Also, $u_0^* = 0 = \bar{u}_0(-P_2, Q)$, $u_1^* = 1 = \bar{v}_0(-P_2, Q)$, $u_2^* = 1 = \bar{u}_2(-P_2, Q)$, $u_3^* = -P_2 - 3Q = \bar{v}_3(-P_2, Q)$. It follows that if $QT_{-1} = 1$, then

$$T_n = \begin{cases} T_2 u_n^*, & \text{if } 2 \mid n; \\ u_n^*, & \text{if } 2 \nmid n \end{cases}$$

and therefore (T_n) is an odd divisibility sequence when we replace Q by $-Q$.

As an example of this consider $Q = -1$, $P_2 = -1$. We have $T_0 = 0$, $T_1 = 1$, $T_2 = 1$, $T_3 = 4$,

$$T_{n+4} = 3T_{n+2} - T_n \quad \text{(see Sloane [7, A005013])}$$

and $T_n = T_{-n}$. Furthermore,

$$T_n = \begin{cases} F_n, & \text{if } 2 \mid n; \\ L_n, & \text{if } 2 \nmid n, \end{cases} \tag{8}$$

where F_n and L_n denote the n^{th} Fibonacci and Lucas numbers, respectively. Also, $T_n = \bar{u}_n(5, 1)$.

Let $\Delta = SU^2$ and $E = GV^2$, where S, G, U, V are integers and S and G are both non-zero and square-free. Let (T_n) be any non-null linear divisibility sequence with characteristic polynomial $F(x)$ given by (2) with $D \neq 0$ and $P_1 \neq 0$. In [12] the following results are proved:

- There is one and only one even (T_n) for any given $F(x)$;
- If $S \neq 1$ and $G \neq 1$, (T_n) is either even or odd;
- If $S \neq 1$ and $G \neq 1$ and $G \neq S$, there can be no odd (T_n);
- If $S = 1$ and $G \neq 1$, then the only possible odd (T_n) is a Lucas sequence (u_n).

We can now partition the possible cases for which (T_n) can be an odd divisibility sequence as follows:

(i) $S = G \neq 1$;

(ii) $S = 1$, $G \neq 1$;

(iii) $S \neq 1$, $G = 1$;

(iv) $S = G = 1$.

It is not known whether any (T_n) exist in cases (i) and (iii), but none are known and it seems most unlikely in case (iii).

As the problem of determining all even LDSs of order 4 is solved, we will devote the remainder of the paper to deriving some further properties of odd LDSs of order 4. Also, as a result of our earlier discussion, we may assume that $P_1 \neq 0$. Let (T_n) be any divisibility sequence satisfying (3) and p be any fixed prime such that $p \mid T_n$ for some $n > 0$.

Definition 10. Let ω_1 be the least positive integer such that $p \mid T_{\omega_1}$. We define the increasing sequence $\omega_1, \omega_2, \ldots, \omega_j \in \mathbb{Z}$ by $p \mid T_{\omega_i}$ and $\omega_i \nmid \omega_j$ $(1 \leq i < j)$. Each ω_i in this sequence is called a *rank of appearance*[1] of p.

Definition 11. If $p \mid T_n$ implies that $\omega_1 \mid n$, then p has a single rank of appearance in (T_n). Such a sequence is said to be *monoapparitic* modulo p and the prime p is said to be *monoapparitic* in (T_n).

In [8] Ward proved that primes have only finitely many ranks of appearance in a general LDS. In this paper we shall be concerned with the special case of an odd LDS of order 4.

With the exception of Section 2, we will reserve the notation (A_n) to denote an odd, non-null and non-degenerate LDS of order 4. By [12, Proposition 4.1] we may assume that $\gcd(P_1, P_2, Q) = 1$. The purpose of this paper is to prove Theorem A below.

Theorem A. *Let (A_n) satisfy (3) and let p be any prime such that $p \mid A_n$ for some $n > 1$; p can have at most two ranks of appearance in (A_n). If $p \nmid P_1$, then p has only one rank of appearance (is monoapparitic) in (A_n) when $p \mid Q\Delta E$. It is also monoapparitic if $S = 1$, $G \neq 1$; $S \neq 1$, $G = 1$; or $S = G \neq 1$. In the case of $S = G = 1$, there are sequences (A_n) for which p $(p \nmid P_1)$ can have two distinct ranks of appearance.*

We will prove Theorem A by showing that it holds for each of the cases (i)–(iv). In Section 2 we derive a number of useful identity relations connecting (A_n) to some special sequences (X_n), (Y_n), (U_n) and (W_n). We also prove a version of Theorem 3 in the particular case of (A_n). In the following section we provide a number of simple results which allow for the determination of when a prime p is monoapparitic in (A_n) for certain special cases. We also show that in general a prime can have at most two ranks of appearance in (A_n). The remaining sections deal with the problem of when p can be monoapparitic in the cases that remain.

2 Odd divisibility sequences of order 4

We have already seen that odd LDSs of order 4 exist; for example, $(\bar{u}_n(r, q))$ is such a sequence. Furthermore, the sequences A215466 and A127595 in the *On-line Encyclopedia of Integer Sequences* (OEIS) (see Sloane [7]) are examples of odd LDSs of order 4 which are not Lehmer sequences. In what follows we will derive some results which must be true for (A_n) if (A_n) is simply an odd linear recurrence sequence of order 4. In the first part of this section we will develop some of the machinery needed throughout the paper. We then use these results to prove the main result of the section: Theorem 13. This theorem is a more

[1] Lucas used the term "le rang d'apparition" and the French word "apparition" has been–and still is–widely used among English writers. However, it is best to avoid the ghostly or miraculous connotation that the English word "apparition" possesses and use "appearance" instead.

specialized version of Theorem 3 and helps in discerning when (A_n) can and cannot be a divisibility sequence.

We begin, as was done in [10] and [12], by defining the auxiliary sequences (W_n), (U_n), (X_n) and (Y_n) by

$$v_n(\rho_i, Q) = W_n + \rho_i U_n = \alpha_i^n + \beta_i^n \tag{9}$$

and

$$u_n(\rho_i, Q) = X_n + \rho_i Y_n = \frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i}; \tag{10}$$

here $\rho_i = \alpha_i + \beta_i$ $(i = 1, 2)$. Also, ρ_1, ρ_2 are the distinct roots of $x^2 - P_1 x + P_2 = 0$. We point out here that $X_n = U_{0,n}$, $Y_n = U_{1,n}$, $W_n = V_{0,n}$, $U_n = V_{1,n}$, where the symbols $U_{i,n}$, $V_{i,n}$ $(i = 0, 1)$ are defined in [9, (10.1.5) and (10.1.6)] (with $k = 2$). Notice each of (W_n), (U_n), (X_n), (Y_n) satisfies (3). Also, the initial terms of these sequences are as follows:

$$\begin{array}{lllll}
W_{-1} = 0, & W_0 = 2, & W_1 = 0, & W_2 = -P_2 - 2Q, & W_3 = -P_1 P_2; \\
U_{-1} = \dfrac{1}{Q}, & U_0 = 0, & U_1 = 1, & U_2 = P_1, & U_3 = P_1^2 - P_2 - 3Q; \\
X_{-1} = \dfrac{-1}{Q}, & X_0 = 0, & X_1 = 1, & X_2 = 0, & X_3 = -P_2 - Q; \\
Y_{-1} = 0, & Y_0 = 0, & Y_1 = 0, & Y_2 = 1, & Y_3 = P_1.
\end{array}$$

Further,

$$(X_n), (Y_n), (W_n), (U_n) \subseteq \mathbb{Z} \quad (n \geq 0).$$

By Theorem 8, we see that both (X_n) and (Y_n) are odd. Indeed, we have

$$X_{-n} = -X_n/Q^n, \quad Y_{-n} = -Y_n/Q^n.$$

Also,

$$W_{-n} = W_n/Q^n, \quad U_{-n} = U_n/Q^n,$$

thus (W_n), (U_n) are even.

In [12] it is noted that if (A_n) is a LDS of order 4, then

$$A_n = X_n + A_2 Y_n; \tag{11}$$

however, this condition is not sufficient for (A_n) to be such a sequence. From Theorem 3 we can derive the following result.

Proposition 12. *For (A_n) defined as above we must have*

$$A_n \mid Q^{n-1} J Y_n^2 U_n^2,$$

where $J = A_2^2 - P_1 A_2 + P_2$.

Proof. By Theorem 3, we know that A_n must be a divisor of r_n for all $n \geq 0$, where here

$$r_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} \cdot \frac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1} \cdot \frac{\alpha_1^n - \beta_2^n}{\alpha_1 - \beta_2} \cdot \frac{\alpha_2^n - \beta_1^n}{\alpha_2 - \beta_1} \cdot \frac{\alpha_2^n - \beta_2^n}{\alpha_2 - \beta_2} \cdot \frac{\beta_1^n - \beta_2^n}{\beta_1 - \beta_2}. \tag{12}$$

Since

$$(\rho_1 - \rho_2)U_n = \alpha_1^n + \beta_1^n - \alpha_2^n - \beta_2^n,$$

we find from (6), that

$$(\rho_1 - \rho_2)U_n = \frac{(\alpha_1^n - \alpha_2^n)(\alpha_2^n - \beta_1^n)}{\alpha_2^n} = \frac{(\beta_1^n - \beta_2^n)(\beta_2^n - \alpha_1^n)}{\beta_2^n}.$$

Hence,

$$Q^n(\rho_1 - \rho_2)^2 U_n^2 = (\alpha_1^n - \alpha_2^n)(\beta_1^n - \beta_2^n)(\alpha_2^n - \beta_1^n)(\beta_2^n - \alpha_1^n);$$

also, for $n = 1$,

$$Q(\rho_1 - \rho_2)^2 = (\alpha_1 - \alpha_2)(\beta_1 - \beta_2)(\alpha_2 - \beta_1)(\beta_2 - \alpha_1).$$

Thus,

$$Q^{n-1}U_n^2 = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} \cdot \frac{\beta_1^n - \beta_2^n}{\beta_1 - \beta_2} \cdot \frac{\alpha_2^n - \beta_1^n}{\alpha_2 - \beta_1} \cdot \frac{\beta_2^n - \alpha_1^n}{\beta_2 - \alpha_1}.$$

By (10), we have

$$\frac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1} \cdot \frac{\alpha_2^n - \beta_2^n}{\alpha_2 - \beta_2} = (X_n + \rho_1 Y_n)(X_n + \rho_2 Y_n) = X_n^2 - P_1 X_n Y_n + P_2 Y_n^2.$$

From these results and (11) we find that,

$$\begin{aligned} r_n &= Q^{n-1}((A_n - A_2 Y_n)^2 - P_1(A_n - A_2 Y_n)Y_n + P_2 Y_n^2)U_n^2 \\ &= Q^{n-1}(A_n^2 - (2A_2 + P_1)A_n Y_n + J Y_n^2)U_n^2, \end{aligned}$$

where $J = A_2^2 - P_1 A_2 + P_2$ and r_n satisfies (12). Thus, we find that

$$A_n \mid Q^{n-1} J Y_n^2 U_n^2 \quad (\text{for all } n \geq 0).$$

□

Later in this section we will improve this result showing that (A_n) is a divisibility sequence if and only if

$$A_n \mid J Y_n U_n \quad (\text{for all } n \geq 0).$$

We will next establish some identities involving the sequences (A_n), (X_n), (Y_n), (W_n), (U_n). We begin with the well-known identity

$$(\alpha_i^n + \beta_i^n)^2 - (\alpha_i - \beta_i)^2 \left(\frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i} \right)^2 = 4\alpha_i^n \beta_i^n = 4Q^n, \tag{13}$$

and get

$$(W_n + \rho_i U_n)^2 - (\rho_i^2 - 4Q)(X_n + \rho_i Y_n)^2 = 4Q^n. \tag{14}$$

Setting $n = 1$ in (13) yields $(\alpha_i - \beta_i)^2 = (\alpha_i + \beta_i)^2 - 4\alpha_i\beta_i = \rho_i^2 - 4Q$. Since $\rho_i^2 = P_1\rho_i - P_2$, we get

$$\begin{gathered}\rho_i^2 - 4Q = P_1\rho_i - P_2 - 4Q,\\ \rho_i(\rho_i^2 - 4Q) = \rho_i(P_1\rho_i - P_2 - 4Q) = (P_1^2 - P_2 - 4Q)\rho_i - P_1P_2,\\ \rho_i^2(\rho_i^2 - 4Q) = \rho_i^2(P_1\rho_i - P_2 - 4Q) = P_1(P_1^2 - P_2 - 4Q)\rho_i - P_2(P_1^2 - P_2 - 4Q).\end{gathered}$$

It follows from (14), that

$$\begin{gathered}W_n^2 - P_2U_n^2 + (P_2 + 4Q)X_n^2 + 2P_1P_2X_nY_n + P_2(P_1^2 - P_2 - 4Q)Y_n^2 = 4Q^n,\\ 2W_nU_n + P_1U_n^2 - P_1X_n^2 - 2(P_1^2 - P_2 - 4Q)X_nY_n - P_1(P_1^2 - 2P_2 - 4Q)Y_n^2 = 0.\end{gathered}$$

From (11), we find by replacing $A_n - A_2Y_n$ for X_n that

$$2W_nU_n + P_1U_n^2 - P_1A_n^2 + 2A_nLY_n - IY_n^2 = 0 \tag{15}$$

and

$$W_n^2 - P_2U_n^2 + (P_2 + 4Q)A_n^2 - 2A_nY_n(A_2(P_2 + 4Q) - P_1P_2) + KY_n^2 = 4Q^n. \tag{16}$$

Here

$$I = P_1A_2^2 - 2(P_1^2 - P_2 - 4Q)A_2 + P_1(P_1^2 - 2P_2 - 4Q), \tag{17}$$

$$K = (P_2 + 4Q)A_2^2 - 2P_1P_2A_2 + P_2(P_1^2 - P_2 - 4Q) \tag{18}$$

and

$$L = P_1A_2 - P_1^2 + P_2 + 4Q. \tag{19}$$

From

$$\begin{aligned}2(X_{n+m} + \rho_i Y_{n+m}) &= 2\left(\frac{\alpha_i^{n+m} - \beta_i^{n+m}}{\alpha_i - \beta_i}\right)\\ &= \left(\frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i}\right)(\alpha_i^m + \beta_i^m) + \left(\frac{\alpha_i^m - \beta_i^m}{\alpha_i - \beta_i}\right)(\alpha_i^n + \beta_i^n)\\ &= (X_n + \rho_i Y_n)(W_m + \rho_i U_m) + (X_m + \rho_i Y_m)(W_n + \rho_i U_n),\end{aligned}$$

so we find that

$$\begin{aligned}2X_{n+m} &= W_nX_m + W_mX_n - P_2(U_nY_m + U_mY_n),\\ 2Y_{n+m} &= U_nX_m + U_mX_n + W_nY_m + W_mY_n + P_1(U_nY_m + U_mY_n).\end{aligned}$$

Multiplying the second of these by A_2 and adding, we see since $A_n = X_n + A_2Y_n$ that

$$2A_{n+m} = W_nA_m + W_mA_n + A_2(U_nA_m + U_mA_n) - J(U_nY_m + U_mY_n). \tag{20}$$

By using

$$\begin{aligned}2(W_{n+m}+\rho_i U_{n+m}) &= 2(\alpha_i^{n+m}+\beta_i^{n+m})\\ &= (\alpha_i^n+\beta_i^n)(\alpha_i^m+\beta_i^m)+(\alpha_i-\beta_i)^2\left(\frac{\alpha_i^n-\beta_i^n}{\alpha_i-\beta_i}\right)\left(\frac{\alpha_i^m-\beta_i^m}{\alpha_i-\beta_i}\right)\\ &= (W_n+\rho_i U_n)(W_m+\rho_i U_m)+(\rho_i^2-4Q)(X_n+\rho_i Y_n)(X_m+\rho_i Y_m),\end{aligned}$$

we get

$$\begin{aligned}2W_{n+m} = W_nW_m - P_2U_nU_m - (P_2+4Q)X_nX_m - P_1P_1(X_nY_m+X_mY_n)\\ - P_2(P_1^2-P_2-4Q)Y_nY_m\end{aligned}$$

and

$$\begin{aligned}2U_{n+m} = U_nW_m+U_mW_n+P_1(U_nU_m+X_nX_m)+(P_1^2-P_2-4Q)(X_nY_m+X_mY_n)\\ + P_1(P_1^2-2P_2-4Q)Y_nY_m.\end{aligned}$$

Once again, using (11), we derive

$$2U_{n+m} = U_nW_m+U_mW_n+P_1(U_nU_m+A_nA_m)-L(A_nY_m+Y_nA_m)+IY_nY_m, \tag{21}$$

where $L = A_2P_1-(P_1^2-P_2-4Q)$. Note the following easily established connection between I, J, K and L:

$$JL+K = A_2I. \tag{22}$$

If we put $m=n$ in (20) we get

$$A_{2n} = A_n(W_n+A_2U_n)-JU_nY_n. \tag{23}$$

Also, from [10] we have

$$U_{2n} = 2U_nW_n+P_1U_n^2 \tag{24}$$

$$= P_1A_n^2-2LA_nY_n+IY_n^2. \tag{25}$$

Since

$$\frac{\alpha_i^{n+m}-\beta_i^{n+m}}{\alpha_i-\beta_i} = (\alpha_i^m+\beta_i^m)\left(\frac{\alpha_i^n-\beta_i^n}{\alpha_i-\beta_i}\right)-Q^m\left(\frac{\alpha_i^{n-m}-\beta_i^{n-m}}{\alpha_i-\beta_i}\right),$$

we have

$$X_{n+m}+\rho_iY_{n+m} = (W_m+\rho_iU_m)(X_n+\rho_iY_n)-Q^m(X_{n-m}+\rho_iY_{n-m})$$

and we find

$$\begin{aligned}X_{n+m} &= W_mX_n-P_2U_mY_n-Q^mX_{n-m},\\ Y_{n+m} &= U_mX_n+W_mY_n+P_1U_mY_n-Q^mY_{n-m}.\end{aligned}$$

It follows from the above and (11)

$$A_{n+m} = A_n(W_m + A_2U_m) - JU_mY_n - Q^mA_{n-m}, \tag{26}$$
$$Y_{n+m} = U_mA_n + Y_n(W_m + (P_1 - A_2)U_m) - Q^mY_{n-m}. \tag{27}$$

Since (A_n) is odd, we have $Q^mA_{n-m} = -Q^nA_{m-n}$ and

$$A_{n+m} = A_n(W_m + A_2U_m) - JU_mY_n + Q^nA_{m-n}. \tag{28}$$

Putting $m = kn$ and $n = n$ in (28), we get

$$A_{(k+1)n} = A_n(W_{kn} + A_2U_{kn}) - JU_{kn}Y_n + Q^nA_{(k-1)n}. \tag{29}$$

We are now able to prove the main result of this section.

Theorem 13. *If (A_n) is an odd recurrence sequence of order 4, then (A_n) is a divisibility sequence if and only if $A_n \mid JU_nY_n$ for all $n \geq 1$.*

Proof. If (A_n) is a divisibility sequence, then $A_n \mid A_{2n}$ which implies $A_n \mid JU_nY_n$ by (23). Next, suppose that $A_n \mid JU_nY_n$. Since it is well known (see [10]) that (U_n) is a divisibility sequence, we know that $U_n \mid U_{kn}$ for any $k \geq 0$. Thus, by (29) we have

$$A_{(k+1)n} \equiv Q^nA_{(k-1)n} \pmod{A_n} \quad (k \geq 1).$$

Hence, if $A_n \mid A_{(k-1)n}$, then $A_n \mid A_{(k+1)n}$. Since $A_n \mid A_n$ and, by (23), $A_n \mid A_{2n}$, we find by induction that $A_n \mid A_{mn}$ for any $m \geq 0$. □

Corollary 14. *If (A_n) is an odd LDS of order 4, then $A_2 \mid P_1P_2$.*

Proof. Follows easily from the theorem and the simple fact that $J \equiv P_2 \pmod{A_2}$. □

3 Monoapparitic primes in odd divisibility sequences of order 4

We now let (A_n) denote an odd, non-null, and non-degerate LDS of order 4. The purpose of much of this section is to identify certain monoapparitic primes in (A_n). If all primes are monoapparitic in (A_n), we say that (A_n) is monoapparitic. We observe by attempting all possible values for P_1, P_2, Q, A_2 modulo 2 that only in the case of $2 \mid P_1$, $2 \nmid P_2Q$, $2 \mid A_2$ is it possible for 2 to not be monoapparitic in (A_n). In this case we see that $2 \mid I$, where I is given by (17), $\omega_1 = 2$ and $\omega_2 = 3$.

We begin with the simple result below.

Proposition 15. *If m is a positive integer and $m \mid J$, where $J = A_2^2 - P_1A_2 + P_2$, then $A_n \equiv u_n(A_2, Q) \pmod{m}$.*

Proof. We have $A_0 = 0 = u_0(A_2, Q)$, $A_1 = 1 = u_1(A_2, Q)$, $A_2 = u_2(A_2, Q)$, $A_3 = X_3 + A_2Y_3 = P_1A_2 - P_2 - Q \equiv A_2^2 - Q = u_3(A_2, Q) \pmod{m}$. Also, since

$$Qu_k(A_2, Q) = A_2u_{k+1}(A_2, Q) - u_{k+2}(A_2, Q),$$

we get

$$Qu_{k+1} = A_2u_{k+2} - u_{k+3}, \quad Q^2u_k = QA_2u_{k+1} - Qu_{k+2} = (A_2^2 - Q)u_{k+2} - A_2u_{k+3}.$$

Here we use u_k to denote $u_k(A_2, Q)$. It follows that

$$P_1Qu_{k+1} - Q^2u_k = (P_1A_2 - A_2^2 + Q)u_{k+2} - (P_1 - A_2)u_{k+3}. \tag{30}$$

Now suppose for some $k \geq 0$, we have $A_{k+i} \equiv u_{k+i}(A_2, Q) \pmod{m}$ $(i = 0, 1, 2, 3)$; this is certainly true for $k = 0$. By (3), we get

$$\begin{aligned} A_{k+4} &\equiv P_1u_{k+3} - (P_2 + 2Q)u_{k+2} + P_1Qu_{k+1} - Q^2u_k \\ &= P_1u_{k+3} - (P_2 + 2Q)u_{k+2} + (P_1A_2 - A_2^2 + Q)u_{k+2} - (P_1 - A_2)u_{k+3} \\ &= A_2u_{k+3} - (P_2 + 2Q - P_1A_2 + A_2^2 - Q)u_{k+2} \\ &\equiv A_2u_{k+3} - Qu_{k+2} = u_{k+4} \pmod{m}, \end{aligned}$$

by (30) and $J = A_2^2 - P_1A_2 + P_2 \equiv 0 \pmod{m}$. The result now follows by induction. □

Corollary 16. *If $p \mid J$, then p is monoapparitic in (A_n).*

Proof. If $p \mid J$, then by Proposition 15 we have $A_n \equiv u_n(A_2, Q) \pmod{p}$. We must have p a monoapparitic prime in (A_n) because $(u_n(A_2, Q))$ has at most one rank of appearance modulo p. □

We next turn to the problem of $p \mid Q$. We see that from (3) that each of (X_n), (Y_n) and (U_n) satisfies

$$T_{n+2} \equiv P_1T_{n+1} - P_2T_n \pmod{p} \quad (n \geq 2).$$

By the initial conditions for (X_n), (Y_n) and (U_n) and mathematical induction, it is easy to show that

$$\begin{aligned} Y_n &\equiv u_{n-1}(P_1, P_2) \pmod{p} \quad (n \geq 1), \\ X_n &\equiv -P_2u_{n-2}(P_1, P_2) \pmod{p} \quad (n \geq 2), \\ U_n &\equiv u_n(P_1, P_2) \pmod{p} \quad (n \geq 0). \end{aligned}$$

It follows that

$$A_n = X_n + A_2Y_n \equiv A_2u_{n-1} - P_2u_{n-2} \pmod{p} \quad (n \geq 2),$$

where we now use u_n to denote $u_n(P_1, P_2)$. Observe that since $u_{n-1}^2 - u_{n-2}u_n = P_2^2$, we must have $p \mid P_2$ if $p \mid \gcd(u_n, u_{n-1})$ or $p \mid \gcd(u_{n-1}, u_{n-2})$. However, when $p \mid P_2$, it is easy to show that $u_n \equiv P_1^{n-1} \pmod{p}$; hence $p \mid P_1$, which since $\gcd(P_1, P_2, Q) = 1$, is impossible. Thus, $\gcd(u_n, u_{n-1}) = 1$ and $\gcd(P_2, u_n) = 1$ for all $n \geq 1$, when $p \mid Q$. We can now prove the following proposition.

Proposition 17. *If p be a prime such that $p \mid Q$, then p must be monoapparitic in (A_n).*

Proof. By Theorem 13, we must have $A_n \mid JY_nU_n$ for all $n \geq 1$. If $p \mid A_n$, then $p \mid J$ means that p is monoapparitic in (A_n). If $p \nmid JY_n$, then $p \mid U_n$ which means that $p \mid u_n(P_1, P_2)$ and

$$P_1u_{n-1} - P_2u_{n-2} \equiv 0 \pmod{p}.$$

Also, $p \mid A_n$ implies that

$$A_2u_{n-1} - P_2u_{n-2} \equiv 0 \pmod{p}.$$

Hence, $p \mid (A_2 - P_1)u_{n-1}$. Since, $p \nmid u_{n-1}$, we get $p \mid A_2 - P_1$, but in this case we get $A_n \equiv u_n(P_1, P_2) \pmod{p}$, which means that p is monoapparitic in (A_n). If $p \mid Y_n$, then $p \mid u_{n-1}$, which since $p \mid A_n$ means that $p \mid P_2u_{n-2}$. If $p \nmid P_2$, then $p \mid u_{n-2}$, which is impossible. If $p \mid P_2$, then $p \mid \gcd(P_2, u_{n-1})$ and $\gcd(u_{n-1}, u_n) \neq 1$, which is also impossible. □

We next define two sequences (G_n) and (H_n):

$$G_n = \gcd(A_n, Y_n) \quad \text{and} \quad H_n = \gcd(A_n, U_n).$$

Note that since $A_n = X_n + A_2Y_n$, we have $G_n = \gcd(X_n, Y_n)$. By [9, Lemma 10.3.8], we know that (G_n) is a divisibility sequence, but not necessarily a LDS.

Proposition 18. *For G_n and H_n defined as above, we have* $\gcd(G_n, Q) = 1$. *Also,* $\gcd(H_n, Q) = 1$ *when* $\gcd(A_2 - P_1, Q) = 1$

Proof. The first result follows from [9, Lemma 10.3.9]. Next, suppose that p is any prime such that $p \mid Q$ and $p \mid H_n$. Referring to the proof of Proposition 17, we find that we must have $p \mid A_2 - P_1$, which means that $\gcd(A_2 - P_1, Q) \neq 1$. □

If p is any prime, let $\rho = \rho(p)$ denote the least positive integer value of n (if it exists) such that $p \mid G_n$.

Theorem 19. *If p is any prime such that $p \mid G_n$, then $\rho \mid n$.*

Proof. This proof can be found in [9, Theorem 10.3.13]. □

We will next obtain a somewhat similar result for (H_n). By making use of the identity

$$\alpha_i^{n+m} + \beta_i^{n+m} = (\alpha_i^n + \beta_i^n)(\alpha_i^m + \beta_i^m) - Q^m(\alpha_i^{n-m} + \beta_i^{n-m}),$$

we can easily derive

$$\begin{aligned} W_{m+n} &= W_mW_n - P_2U_mU_n - Q^mW_{n-m}, \\ U_{m+n} &= W_mU_n + W_nU_m + P_1U_nU_m - Q^mU_{n-m}. \end{aligned} \tag{31}$$

From (23) and (24), we see that

$$H_n \mid H_{2n}.$$

By (31) and (29), we have

$$U_{(k+1)n} = W_{kn}U_n + W_nU_{kn} + P_1U_{kn}U_n - Q^nU_{(k-1)n},$$
$$A_{(k+1)n} = A_n(W_{kn} + A_2U_{kn}) - JU_{kn}Y_n + Q^nA_{(k-1)n}.$$

Since $H_n \mid H_n$ and $H_n \mid H_{2n}$, it is easy to establish by induction on m that $H_n \mid H_{mn}$; thus, (H_n) is a divisibility sequence.

For any fixed prime p, let $\sigma = \sigma(p)$, if it exists, be the least positive value of n such that $p \mid H_n$. If $p \mid Q$ and $p \mid H_n$, then as we have seen earlier $p \mid u_n(P_1, P_2)$ and $A_n \equiv U_n \equiv u_n(P_1, P_2) \pmod{p}$ $(p \mid Q)$. Thus, if $p \mid H_n$, then $\sigma \mid n$. We next show that if p is any odd prime such that $p \nmid Q$, then $\sigma \mid n$ whenever $p \mid H_n$.

Theorem 20. *Let p be any odd prime such that $p \nmid Q$. If $p \mid H_n$, then $\sigma(p) \mid n$.*

Proof. We first note that by (15) we have $H_n \mid IY_n^2$ for any n. Suppose $p \mid H_n$ and $n = q\sigma + r$ with $0 < r < \sigma$. From (21) and (20) we have

$$2U_n = U_{q\sigma}W_r + W_{q\sigma}U_r + P_1(U_{q\sigma}U_r + A_{q\sigma}A_r) - L(A_{q\sigma}Y_r + Y_{q\sigma}A_r) + IY_{q\sigma}Y_r$$

and

$$2A_n = W_{q\sigma}A_r + A_{q\sigma}W_r + A_2(U_{q\sigma}A_r + A_{q\sigma}U_r) - J(U_{q\sigma}Y_r + Y_{q\sigma}U_r).$$

Since (H_n) is a divisibility sequence and $p \mid H_\sigma$ $(\sigma = \sigma(p))$ we must have $p \mid H_{q\sigma}$ and $p \mid IY_{q\sigma}$. Thus,

$$0 \equiv W_{q\sigma}U_r - LY_{q\sigma}A_r \pmod{p},$$
$$0 \equiv W_{q\sigma}A_r - JY_{q\sigma}U_r \pmod{p}.$$

If $p \nmid I$, then $p \mid Y_{q\sigma}$, $p \mid W_{q\sigma}U_r$ and $p \mid W_{q\sigma}A_r$; consequently if $p \nmid W_{q\sigma}$, we get $p \mid H_r$. If $p \mid W_{q\sigma}$, then by (16) we get $p \mid 4Q^{q\sigma}$, which is impossible by selection of p. If $p \mid I$, then by (22) and (16), we get

$$W_{q\sigma}^2 - LJY_{q\sigma}^2 \equiv W_{q\sigma}^2 + KY_{q\sigma}^2 \equiv 4Q^{q\sigma} \pmod{p}.$$

Since $p \nmid 4Q^{q\sigma}$, we must also have $p \mid H_r$. In either case we find that we get a contradiction to the definition of σ when $r > 0$. Hence, $\sigma(p) \mid n$. □

We next address the question of the existence of $\rho(p)$ and $\sigma(p)$. We will only concern ourselves with those primes p such that p divides some term A_n $(n > 0)$ of (A_n) and $p \nmid J$. By Theorem 13, we must have $p \mid G_n$ or $p \mid H_n$; thus, at least one of $\rho(p)$ or $\sigma(p)$ must exist. From (23) and (25), we can easily deduce that

$$G_n \mid H_{2n}; \tag{32}$$

hence, if $\rho(p)$ exists, then $p \mid H_{2\rho}$ and therefore $\sigma(p)$ must exist. Also, even if $\rho(p)$ does not exist, then $\sigma(p)$ must exist and p is monoapparitic in (A_n). Since $\gcd(G_n, Q) = 1$, we see

that if $p \mid Q$, then $\rho(p)$ cannot exist. Also, if $p \mid Q$ and $A_2 \not\equiv P_1 \pmod{p}$, then $p \nmid H_n$ and as a result $\sigma(p)$ cannot exist.

We will now examine several additional special cases. Throughout this discussion p will denote a prime such that $p \nmid 2Q$.

Case 1: $p \mid P_1$**.**

In this case, it is easy to prove by using (3) and mathematical induction that for $n \geq 0$ we have

$$X_{2n} \equiv 0, \quad X_{2n+1} \equiv \bar{u}_n(-P_2, Q), \quad Y_{2n} \equiv \bar{u}_{2n}(-P_2, Q), \quad Y_{2n+1} \equiv 0 \pmod{p}. \tag{33}$$

Hence, $G_n = \gcd(X_n, Y_n) \equiv \bar{u}_n(-P_2, Q) \pmod{p}$. By results in [4] (See §4 below for details.) we know that if $p \nmid P_2$, then $p \mid \bar{u}_n(-P_2, Q)$ if and only if $\tau \mid n$, where τ is the rank of appearance of p in $(\bar{u}_n(-P_2, Q))$. Since $p \nmid Q$, τ must exist and $\tau \mid p - \kappa$, where κ is the value of the Legendre symbol $((P_2^2 + 4QP_2)/p)$. Hence, $\rho(p)$ exists and $\rho(p) = \tau$ when $p \nmid P_2$. Suppose $p \mid P_2$; then $p \nmid \bar{u}_n(-P_2, Q)$ for any odd $n > 0$ and $\rho(p)$ does not exist. If $2 \mid n$, then $p \mid (\bar{u}_n(-P_2, Q))$ if and only if $p \mid n$; hence, $\rho(p) = \tau = p$ in this case.

Proposition 21. *If $p \mid P_1$, then p is monoapparitic in (A_n) when $p \nmid A_2$. If $p \mid P_1$, $p \mid A_2$ and $2 \mid \tau$, then p is also monoapparitic in (A_n). If $p \mid P_1$, $p \mid A_2$ and $2 \nmid \tau$, it is possible for p to have two ranks of appearance in (A_n), namely 2 and τ. Also, if $p \mid P_1$, $p \mid A_2$ and $p \mid P_2$, then p is monoapparitic in (A_n).*

Proof. If $p \mid P_1$, $p \mid A_2$ and $p \mid P_2$, then $p \mid J$ and therefore p is monoapparitic in (A_n) by Corollary 16. Furthermore, by (33) we have

$$A_n = \begin{cases} \bar{u}_n(-P_2, Q), & \text{if } 2 \nmid n; \\ A_2 \bar{u}_n(-P_2, Q), & \text{if } 2 \mid n. \end{cases}$$

The result now easily follows from our observations in **Case 1**. □

Case 2: $p \nmid P_1$**,** $p \mid \Delta$**.**

In [10, §6] it is shown that

$$U_n \equiv n u_n(P_1/2, Q) \pmod{p}.$$

Also, it is easy, on using the initial conditions for (X_n) and (Y_n), to see that

$$X_n + (P_1/2)Y_n \equiv u_n(P_1/2, Q) \pmod{p} \tag{34}$$

for $n = 0, 1, 2, 3$. On putting $P_2 \equiv P_1^2/4 \pmod{p}$, we use (3) and mathematical induction to verify that (34) is true for all $n \geq 1$. Thus, if $p \mid G_n$, then $p \mid H_n$. Hence, if $\rho(p)$ exists, then $\sigma(p)$ exists and $\sigma(p) \mid \rho(p)$ by Theorem 20.

Case 3: $p \nmid P_1\Delta$, $p \mid E$.

We first observe by [12, (2.5)] we have

$$\Delta P_1^2 + 4E = (P_1^2 - 2P_2 - 8Q)^2; \tag{35}$$

thus, since $p \mid E$ and $p \nmid P_1\Delta$, we must have $(\Delta/p) = 1$. Let $\mathbb{K}$ be the splitting field of $F(x)$ in $\mathbb{F}_p[x]$ and let α_1, β_1, α_2, β_2 ($\alpha_1\beta_1 = \alpha_2\beta_2 = Q$) be the roots of $F(x) = 0$ in $\mathbb{K}$. Since $E = (\alpha_1 - \beta_1)^2(\alpha_2 - \beta_2)^2$, we have $\alpha_1 = \beta_1$ or $\alpha_2 = \beta_2$ in $\mathbb{K}$. We assume with no loss of generality that $\alpha_1 = \beta_1$. If, as well, $\alpha_2 = \beta_2$, then since $(\alpha_i - \beta_i)^2 = \rho_i^2 - 4Q$ ($i = 1, 2$), we see that $\rho_1^2 = \rho_2^2$, which since $p \nmid P_1\Delta$ is impossible. Thus $\alpha_1 = \beta_1$ and $\alpha_2 \neq \beta_2$. Also, since $(\Delta/p) = 1$, we must have $\rho_1 - \rho_2 \in \mathbb{F}_p \subseteq \mathbb{K}$ and therefore ρ_1, $\rho_2 \in \mathbb{F}_p$. Since $\alpha_1 = \beta_1$, we have $\rho_1 = 2\alpha_1$. Thus in $\mathbb{F}_p$

$$u_n(\rho_1, Q) = \frac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1} = n\alpha_1^{n-1} \quad \text{and} \quad u_n(\rho_2, Q) = \frac{\alpha_2^n - \beta_2^n}{\alpha_2 - \beta_2}.$$

By definition of (X_n) and (Y_n), we find that in $\mathbb{F}_p$

$$X_n + \rho_1 Y_n = n\alpha_1^{n-1} \quad \text{and} \quad X_n + \rho_2 Y_n = u_n(\rho_2, Q).$$

Thus, if $p \mid G_n$, then $n\alpha_1^{n-1} = 0$ and $u_n(\rho_2, Q) = 0$ in $\mathbb{F}_p$. Since $p \nmid Q$, we see that $p \mid n$. Also, by [10, Lemma 8.1] we know that if τ is the rank of appearance of p in $u_n(\rho_2, Q)$, then $\tau \mid n$, where $\tau \mid p - \lambda$ and λ is the value of the Legendre symbol $((P_1^2 - 2P_2 - 8Q)/p)$. Since $\alpha_2 \neq \beta_2$, we cannot have $\lambda = 0$; thus, $\gcd(\tau, p) = 1$ and $p\tau \mid n$. Furthermore, if $p\tau \mid n$, then $X_n + \rho_1 Y_n = X_n + \rho_2 Y_n$ in $\mathbb{F}_p$. Since $\rho_1 - \rho_2 \neq 0$, $Y_n = X_n = 0$ and $p \mid G_n$. It follows that in this case, $\rho(p)$ exists and $\rho(p) = p\tau$.

Finally, we deal with the case of $p \nmid \Delta EQ$. If $(\Delta/p) = 1$, there must exist some d such that $d^2 \equiv \Delta \pmod{p}$. In this case, put $e = P_1^2 - \Delta - 16Q + 2P_1 d$ and η is the value of the Legendre symbol (e/p). We define the function $\Phi(p)$ by

$$\Phi(p) = \begin{cases} p - \eta, & \text{if } (\Delta/p) = 1,\ (E/p) = 1; \\ p^2 - 1, & \text{if } (\Delta/p) = 1,\ (E/p) = -1; \\ p^2 - (E/p), & \text{if } (\Delta/p) = -1. \end{cases}$$

We now have the following result.

Theorem 22. *If p is any odd prime such that $p \nmid \Delta EQ$, then both $\rho = \rho(p)$ and $\sigma = \sigma(p)$ must exist and are divisors of $\Phi(p)$.*

Proof. By [9, Theorem 10.3.10] and results in [10, §7], we know that $p \mid G_{\Phi(p)}$ and $p \mid U_{\Phi(p)}$; hence $p \mid H_{\Phi(p)}$. It follows that both ρ and σ exist for p and by Theorems 19 and 20, we must have $\rho(p) \mid \Phi(p)$ and $\sigma(p) \mid \Phi(p)$, respectively. □

While it is the case that the Lucas sequences have a single rank of appearance, we have seen that higher order divisibility sequences may have multiple ranks of appearance [8]. In the theorem below we now show that (A_n) can have at most two ranks of appearance for any prime p.

Theorem 23. *Any prime p can have at most two ranks of appearance in (A_n).*

Proof. By our previous results we may assume that $p \nmid 2QJ$. If $p \mid A_n$, then by Theorem 13, we must have $p \mid Y_n$ or $p \mid U_n$. That is, $\rho(p) \mid n$ or $\sigma(p) \mid n$. It follows that there can be at most two ranks of appearance of p in (A_n), namely ρ and σ. □

We will next derive some simple conditions under which a prime p must be monoapparitic in (A_n). We have already seen that this will be the case if $p \mid Q$ or $p \mid J$; thus we will assume in what follows that $p \nmid 2QJ$. Let $\omega = \omega_1(p)$, where ω_1 is defined in Definition 10 with $(T_n) = (A_n)$. Put $\rho = \rho(p)$, $\sigma = \sigma(p)$, when they exist. Since $p \mid A_\rho$ and $p \mid A_\sigma$, it is clear that $\omega \leq \rho$ and $\omega \leq \sigma$.

Proposition 24. *For the symbols p, ω, σ and ρ defined above, we have $\omega = \rho$ or $\omega = \sigma$.*

Proof. By Theorems 23, 19 and 20, we must have $\rho \mid \omega$ or $\sigma \mid \omega$. Since $\rho, \sigma \geq \omega$, we can only have $\omega = \rho$ or $\omega = \sigma$. □

Proposition 25. *Under the conditions of Proposition 24, p is monoapparitic in (A_n) when $\sigma \mid \rho$ or $\rho \mid \sigma$.*

Proof. We show that if $p \mid A_n$, then $\omega \mid n$. Suppose $\sigma \mid \rho$. In this case $\sigma \leq \rho$; hence, by Proposition 24 and the definition of ω we must have $\omega = \sigma$. If $p \mid A_n$, then we must have $\sigma \mid n$ or $\rho \mid n$ by Theorem 23, which means that $\sigma \mid n$ and $\omega \mid n$. Similarly, if $\rho \mid \sigma$, then $\omega = \rho$ and $\rho \mid n$. □

Proposition 26. *If $p \nmid P_1$, and $p \mid \Delta$, then p is monoapparitic in (A_n).*

Proof. In **Case 2** we showed that if p satisfies the conditions of the proposition, then either $\rho(p)$ and $\sigma(p)$ both exist and $\sigma \mid \rho$, or $\rho(p)$ does not exist. In either case p must be monoapparitic in (A_n). □

By (32) we see that if $p \mid G_\rho$, we must have $p \mid H_{2\rho}$ and therefore

$$\sigma \mid 2\rho$$

by Theorem 20. It follows that if $2 \nmid \sigma$, then $\sigma \mid \rho$ and p is monoapparitic in (A_n).

Proposition 27. *If $\rho \leq \sigma$, then p is monoapparitic in (A_n).*

Proof. We may assume that $2 \mid \sigma$. Since $\sigma/2 \mid \rho$, we get $\rho = t\sigma/2 \leq \sigma$. Thus, $t = 1, 2$. If $t = 2$, then $\rho = \sigma$ and we are done. If $t = 2$, then $\rho = \sigma/2$. Since $\rho \mid \sigma$, the result follows from Proposition 25. □

Thus, if $\rho \leq \sigma$ or $2 \nmid \sigma$, we see that p is monoapparitic in (A_n). In the following result we present another condition for this to be the case.

Theorem 28. *If $p \nmid I$, then (A_n) has a single rank of appearance modulo p.*

Proof. We may assume that $p \nmid 2QJ$. It suffices to show that if $p \mid A_n$, then $\omega \mid n$. If $p \mid A_n$, then $p \mid U_n$ or $p \mid Y_n$ which means that $p \mid H_n$ or $p \mid G_n$. If $p \mid H_n$, by (15) we see that $p \mid G_n$. Thus, $p \mid G_\omega$ and we must have $\rho \mid \omega$. Since $\omega \leq \rho$, we have $\omega = \rho$. Also, since $p \mid G_n$, we have $\rho \mid n$, which means that $\omega \mid n$. □

We have seen, then, that if $p \nmid I$, p is a monoapparitic prime in (A_n). If $I \neq 0$, this means that only a finite number of primes can have two ranks of appearance in (A_n). In the next section we will deal with the case of $I = 0$ and the case of $p \mid I$.

4 Some results when $I = 0$ or $p \mid I$

Put

$$g = P_1^2 - P_2 - 4Q, \quad h = P_1(P_1^2 - 2P_2 - 4Q) \tag{36}$$

and note that

$$E = g^2 - P_1 h. \tag{37}$$

If $I = 0$, we have from (17) that

$$P_1 A_2^2 - 2gA_2 + h = 0. \tag{38}$$

As mentioned in Section 1, we assume that $P_1 \neq 0$. By (37) the discriminant of

$$P_1 x^2 - 2gx + h = 0$$

is $4E$. Thus, for $A_2 \in \mathbb{Z}$, we see that E must be a perfect integral square, which means that $G = 1$.

In the case of $p \mid I$, we can convert (38) into a congruence modulo p and find that

$$(P_1 A_2 - g)^2 \equiv E \pmod{p}. \tag{39}$$

We are now able to complete our discussion of the special cases that arise when $p \mid D$ in (4).

Proposition 29. *If $p \nmid 2P_1$ and $p \mid E$, then p is monoapparitic in (A_n).*

Proof. Put

$$q \equiv (P_2 + 4Q)/P_1 \pmod{p}.$$

Since $p \mid E$, we have

$$q^2 \equiv 4Q \pmod{p}.$$

by the second formula in (5). From (39), we see that

$$A_2 \equiv P_1 - q \pmod{p};$$

thus,

$$J = A_2^2 - P_1A_2 + P_2 \equiv q^2 - P_1q + P_2 \equiv 4Q - (P_2 + 4Q) + P_2 \equiv 0 \pmod{p}.$$

By Corollary 16, p must be monoapparitic in (A_n). □

By combining the results of Propositions 17, 26 and 29, we have the following result.

Theorem 30. *If p is any prime such that $p \nmid 2P_1$ and $p \mid \Delta EQ$, then p is monoapparitic in (A_n).*

We next deal with (A_n) when p is an odd prime and Case (i) of Section 1 holds, i.e., $G = S \neq 1$. We put

$$d = P_1^2 - 2P_2 - 8Q, \quad c = P_1(P_1^2 - 3P_2 - 4Q). \tag{40}$$

By [12, Theorem 5.2] we know that if (A_n) is an odd LDS, then

$$dA_2 = c \pm \sqrt{\Delta E}; \tag{41}$$

thus,

$$d^2A_2^2 - 2cdA_2 + c^2 - \Delta E = 0. \tag{42}$$

In what follows we will assume that $p \nmid P_1$. Since $p \mid I$, by (38) we have

$$P_1A_2^2 - 2gA_2 + h \equiv 0 \pmod{p}. \tag{43}$$

It is easy to verify by referring to (5), (36) and (40) that

$$gd - P_1c = 2E \tag{44}$$

and

$$\Delta P_1h + P_1^2E = c^2. \tag{45}$$

From (42) and (43), we have

$$P_1d^2A_2^2 - 2cdP_1A_2 + P_1(c^2 - \Delta E) \equiv 0 \pmod{p}$$

and

$$P_1d^2A_2^2 - 2gd^2A_2 + d^2h \equiv 0 \pmod{p}.$$

On subtracting the second of these congruences from the first we get

$$2d(gd - P_1c)A_2 + P_1(c^2 - \Delta E) - d^2h \equiv 0 \pmod{p}. \tag{46}$$

Now by (45) we have

$$P_1(c^2 - \Delta E) - d^2 h = E(P_1^3 - P_1\Delta - 4h) = -4E(h - P_1P_2) = 4Ec;$$

it follows from this, (46) and (44) that

$$4dEA_2 - 4Ec \equiv 0 \pmod{p}. \tag{47}$$

We are now able to derive the following simple result.

Theorem 31. *If p is a prime such that $p \nmid 2P_1$, then p is monoapparitic in (A_n) when $S = G \neq 1$.*

Proof. By Theorem 30, we see that the theorem holds when $p \mid \Delta E$. Suppose $p \nmid \Delta E$ and $p \mid I$. If $p = 2$ and $p \nmid P_1$, then we have already seen that p is monoapparitic in (A_n). Thus, we may assume here that $p \neq 2$. By (47), we get

$$dA_2 - c \equiv 0 \pmod{p}$$

and by (41) we must have $p \mid \Delta E$, a contradiction. Thus p must be monoapparitic in (A_n). □

In [11], it is shown that if $G = 1$, there must exist integers r_1, r_2, q_1, q_2 such that r_1, $r_2 > 0$; $\gcd(r_1, q_1) = \gcd(r_2, q_2) = 1$;

$$P_1^2 = r_1 r_2, \quad P_2 = q_1 r_2 + q_2 r_1 - 4q_1 q_2, \quad Q = q_1 q_2. \tag{48}$$

We find that $\Delta = P_1^2 - 4P_2 = d_1 d_2$, where $d_i = r_i - 4q_i$ $(i = 1, 2)$, $E = (q_1 r_2 - q_2 r_1)^2$ and $g = r_1 r_2 - r_1 q_2 - r_2 q_1$. It is also shown in [11] that for the values of P_1, P_2, Q given by (48), we have

$$\alpha_1 = \mu_1\mu_2, \quad \beta_1 = \nu_1\nu_2, \quad \alpha_2 = \nu_1\mu_2, \quad \beta_2 = \mu_1\nu_2,$$

where $\mu_i + \nu_i = \sqrt{r_i}$, $\mu_i\nu_i = q_i$ $(i = 1, 2)$. Since $\mu_1/\nu_1 = \alpha_1/\alpha_2$ and $\mu_2/\nu_2 = \alpha_2/\beta_1$, we see that since (A_n) is non-degenerate, we cannot have μ_1/ν_1 or μ_2/ν_2 a root of unity; in particular $\mu_1 \neq \nu_1$ and $\mu_2 \neq \nu_2$.

We next observe that

$$(\alpha_1^n - \beta_1^n) + (\alpha_2^n - \beta_2^n) = \mu_1^n\mu_2^n - \nu_1^n\nu_2^n + \mu_1^n\nu_2^n - \mu_2^n\nu_1^n = (\mu_1^n - \nu_1^n)(\mu_2^n + \nu_2^n) \tag{49}$$

$$(\alpha_1^n - \beta_1^n) - (\alpha_2^n - \beta_2^n) = (\mu_1^n + \nu_1^n)(\mu_2^n - \nu_2^n). \tag{50}$$

Put

$$M_n = u_n(\sqrt{r_1}, q_1)v_n(\sqrt{r_2}, q_2), \quad N_n = v_n(\sqrt{r_1}, q_1)u_n(\sqrt{r_2}, q_2).$$

We have

$$(\mu_1^n - \nu_1^n)(\mu_2^n + \nu_2^n) = (\mu_1 - \nu_1)M_n, \quad (\mu_1^n + \nu_1^n)(\mu_2^n - \nu_2^n) = (\mu_2 - \nu_2)N_n.$$

Also, by (49) and (50) and the definition of (X_n), (Y_n), we get

$$(\alpha_1-\beta_1)X_n+(\alpha_1-\beta_1)\rho_1Y_n+(\alpha_2-\beta_2)X_n+(\alpha_2-\beta_2)\rho_2Y_n=(\mu_1-\nu_1)M_n,$$
$$(\alpha_1-\beta_1)X_n+(\alpha_1-\beta_1)\rho_1Y_n-(\alpha_2-\beta_2)X_n-(\alpha_2-\beta_2)\rho_2Y_n=(\mu_2-\nu_2)N_n.$$

Since $\rho_i=\alpha_i+\beta_i$ $(i=1,2)$, we see, by (49) and (50) with $n=2$, that

$$(\alpha_1-\beta_1)\rho_1+(\alpha_2-\beta_2)\rho_2=(\mu_1^2-\nu_1^2)(\mu_2^2+\nu_2^2)$$

and

$$(\alpha_1-\beta_1)\rho_1-(\alpha_2-\beta_2)\rho_2=(\mu_1^2+\nu_1^2)(\mu_2^2-\nu_2^2).$$

It follows that

$$\sqrt{r_2}X_n+\sqrt{r_1}(r_2-2q_2)Y_n=M_n, \tag{51}$$
$$\sqrt{r_1}X_n+\sqrt{r_2}(r_1-2q_1)Y_n=N_n. \tag{52}$$

From [11], we also have

$$U_n=u_n(\sqrt{r_1},q_1)u_n(\sqrt{r_2},q_2).$$

If we put

$$R_n=\bar{u}_n(r_1,q_1)\bar{v}_n(r_2,q_2),\quad S_n=\bar{u}_n(r_2,q_2)\bar{v}_n(r_1,q_1),$$

we get

$$M_n=\sqrt{r_2}R_n,\quad N_n=\sqrt{r_1}S_n\quad \text{if } 2\nmid n,$$
$$M_n=\sqrt{r_1}R_n,\quad N_n=\sqrt{r_2}S_n\quad \text{if } 2\mid n,$$

and

$$U_n=\begin{cases}\bar{u}_n(r_1,q_1)\bar{u}_n(r_2,q_2), & \text{if } 2\nmid n;\\ P_1\bar{u}_n(r_1,q_1)\bar{u}_n(r_2,q_2), & \text{if } 2\mid n.\end{cases} \tag{53}$$

If $I=0$, then with a possible interchange of the parameters r_1, r_2 and q_1, q_2, we get

$$A_2=\frac{g\pm\sqrt{E}}{P_1}=\sqrt{r_1r_2}-2q_1\sqrt{\frac{r_2}{r_1}}=v_2(\sqrt{r_1},q_1)\frac{u_2(\sqrt{r_2},q_2)}{\sqrt{r_1}}.$$

Notice that

$$A_{-1}=\frac{-1}{Q}=v_{-1}(\sqrt{r_1},q_1)\frac{u_{-1}(\sqrt{r_2},q_2)}{\sqrt{r_1}},$$
$$A_0=0=v_0(\sqrt{r_1},q_1)\frac{u_0(\sqrt{r_2},q_2)}{\sqrt{r_1}},$$
$$A_1=1=v_1(\sqrt{r_1},q_1)\frac{u_1(\sqrt{r_2},q_2)}{\sqrt{r_1}};$$

thus, if we put

$$B_n = v_n(\sqrt{r_1}, q_1)\frac{u_n(\sqrt{r_2}, q_2)}{\sqrt{r_1}} = N_n/\sqrt{r_1},$$

we have $A_i = B_i$ $(i = -1, 0, 1, 2)$. Since α_1, β_1, α_2, β_2 are the distinct roots of (2), we see that the sequence (B_n) given by

$$B_n = \left(\frac{\mu_1^n + \nu_1^n}{\mu_1 + \nu_1}\right)\left(\frac{\mu_2^n - \nu_2^n}{\mu_1 - \nu_1}\right) = \frac{\alpha_1^n - \beta_1^n + \alpha_2^n - \beta_2^n}{\alpha_1 - \beta_1 + \alpha_2 - \beta_2}$$

must satisfy (3). Since the initial values of (B_n) and (A_n) are equal, it follows that

$$A_n = B_n = v_n(\sqrt{r_1}, q_1)\frac{u_n(\sqrt{r_2}, q_2)}{\sqrt{r_1}} = \begin{cases} \bar{v}_n(r_1, q_1)\bar{u}_n(r_2, q_2), & \text{if } 2 \nmid n; \\ \dfrac{r_2}{P_1}\bar{v}_n(r_1, q_1)\bar{u}_n(r_2, q_2), & \text{if } 2 \mid n, \end{cases} \tag{54}$$

when $I = 0$. Also, if $p \nmid P_1QE$, $G = 1$ and $p \mid I$, we can use (39) and the above reasoning to show that

$$A_n \equiv \begin{cases} \bar{v}_n(r_1, q_1)\bar{u}_n(r_2, q_2) \pmod{p}, & \text{if } 2 \nmid n; \\ \dfrac{r_2}{P_1}\bar{v}_n(r_1, q_1)\bar{u}_n(r_2, q_2) \pmod{p}, & \text{if } 2 \mid n. \end{cases} \tag{55}$$

Thus, by Theorem 31 we have disposed of Case (i) in Section 1. Since in Case (ii), (A_n) is the Lucas sequence (u_n), we see that p must also be monoapparitc in (A_n). This leaves only the two cases when $G = 1$. We deal with the first of these in the next section.

5 The case of $G = 1$ and $S \neq 1$

Before proceeding any further, we will need to review some simple properties of the Lehmer sequences $(\bar{u}_n(r, q))$ and $(\bar{v}_n(r, q))$. We have the simple identities

$$\bar{u}_{2n} = \bar{v}_n\bar{u}_n \tag{56}$$

and

$$\begin{cases} r\bar{v}_n^2 - d\bar{u}_n^2 = 4q^n, & \text{if } 2 \nmid n; \\ \bar{v}_n^2 - rd\bar{u}_n^2 = 4q^n, & \text{if } 2 \mid n. \end{cases} \tag{57}$$

where $d = r - 4q$ and we use $\bar{u}_n$ and $\bar{v}_n$ to represent $\bar{u}_n(r, q)$ and $\bar{v}_n(r, q)$, respectively. If $2 \nmid n$, it is easy to prove

$$\bar{u}_n(mr, mq) = m^{\frac{n-1}{2}}\bar{u}_n(r, q) \tag{58}$$

and

$$\bar{u}_n(r - 4q, q) = \bar{v}_n(r, q). \tag{59}$$

Also, from results in [4] the sequence $(\bar{u}_n(r, q))$ is a fourth-order linear divisibility sequence as is $(a_n\bar{u}_n(r, q))$, where (a_n) is a special periodic sequence of integers such that $a_1 = 1$ and

$a_n \mid a_{2n}$. Indeed, the sequence (a_n) must be some $(\bar{v}_n(r,q))$, where $q = \pm 1$ and $r = q$, $2q$ or $3q$.

Let $\tau = \tau(p)$ be the rank of appearance (apparition) of a prime p ($p \nmid 2rq$) in $(\bar{u}_n(r,q))$. Note that $p \mid \bar{u}_n \Leftrightarrow \tau \mid n$ ([4, Theorem 1.8]). We use $\psi = \psi(p)$ to denote the least positive value of n, if it exists, such that $p \mid \bar{v}_n$. We have two simple results.

Theorem 32. *If $p \nmid 2rq$, then ψ exists if and only if $2 \mid \tau$; furthermore, if $2 \mid \tau$, then $\psi = \tau/2$.*

Proof. Suppose $2 \mid \tau$; by definition of τ we see that $p \nmid \bar{u}_{\tau/2}$ and by (56) $p \mid \bar{v}_{\tau/2}$. Thus, ψ exists and $\psi \leq \tau/2$. Also, by (56), we have $p \mid \bar{u}_{2\psi}$ and therefore $\tau \mid 2\psi \Rightarrow \tau/2 \mid \psi \Rightarrow \psi = \tau/2$. Next, assume that ψ exists; as above, we have $\tau \mid 2\psi$. Also, by (57), we see that $p \nmid \bar{u}_\psi$; hence $\tau \nmid \psi \Rightarrow 2 \mid \tau$. □

Theorem 33. *If $p \nmid 2rq$ and τ is even, then $p \mid v_n \Rightarrow \psi \mid n$. and $2 \nmid n/\psi$.*

Proof. We have $\psi = \tau/2$ exists by Theorem 32. Suppose $p \mid \bar{v}_n$. Since $p \mid \bar{u}_{2n}$, we have $\tau \mid 2n$ and $\tau \nmid n$. Hence, $\psi \mid n$ and since $2\psi \nmid n$, n/ψ is odd. □

It is shown in [12] that if $G = 1$ and $S \neq 1$, then (A_n) is given by (54), where r_1, r_2, q_1 must be perfect integral squares. Put $r_i = s_i^2$ $(i = 1, 2)$. We find that

$$A_n = v_n(s_1, q_1) u_n(s_2, q_2)/s_1 \tag{60}$$

and if (A_n) is to be a divisibility sequence, we must have

$$v_n(s_1, q_1) \mid 2v_n(s_2, q_2) \quad (\text{for all } n \geq 0). \tag{61}$$

Let τ_i be the rank of appearance of the prime p ($p \nmid q_i$) in $(u_n(s_i, q_i))$ $(i = 1, 2)$ and put

$$\omega = \begin{cases} \tau_1/2, & \text{if } 2 \mid \tau_1; \\ \tau_2, & \text{if } 2 \nmid \tau_1. \end{cases}$$

Note that for A_n given by (60), we have $p \mid A_\omega$.

We now have the main result of this section.

Theorem 34. *Let A_n be given by (60), subject to (61). If $p \nmid 2Q$ and $p \mid A_n$, then $\omega \mid n$.*

Proof. If $2 \nmid \tau_1$, then by Theorem 32 $p \nmid v_n(s_1, q_1)$ for any n. Thus by (60) we must have $p \mid u_n(s_2, q_2)$ and $\tau_2 \mid n$. Suppose $2 \mid \tau_1$. If $p \mid v_n(s_1, q_1)$, we must have $\tau_1/2 \mid n$ by Theorem 33. If $p \mid u_n(s_2, q_2)$, then since, $p \mid v_{\tau_1/2}(s_1, q_1)$, we must have $p \mid v_{\tau_1/2}(s_2, q_2)$ by (61). Thus, since ψ_2 must exist, we have $2 \mid \tau_2$ and $\tau_1/2 \mid \tau_2/2$. It follows that since $\tau_2 \mid n$, we get $\tau_1/2 \mid n$. □

It follows from Proposition 17 and Theorem 34 that if $G = 1$, $S \neq 1$ and p is an odd prime, then (A_n) must be monoapparitic modulo p. We have also shown that if $I = 0$ and $S \neq 1$, the primes which can divide the terms of (A_n) must all, with the possible exception of $p = 2$, be monoapparitic.

6 The case of $S = G = 1$

We will first investigate the problem of determining those primes p which can be monoapparitic in (A_n) when all we know is just that $G = 1$. We may assume that $p \nmid 2P_1Q$ and $p \mid I$. If $p \mid U_n$ and $p \mid A_n$, then by (53) and (55) we have

$$p \mid \bar{u}_n(r_1, q_1)\bar{u}_n(r_2, q_2) \quad \text{and} \quad p \mid \bar{v}_n(r_1, q_1)\bar{u}_n(r_2, q_2).$$

Let τ_i $(i = 1, 2)$ be the rank of appearance (apparition) of p in $\bar{u}_n(r_i, q_i)$. Since, by (57), $p \nmid \gcd(\bar{u}_n(r_1, q_1), \bar{v}_n(r_1, q_1))$, we must have $p \mid \bar{u}_n(r_2, q_2)$ and this holds if and only if $\tau_2 \mid n$. Thus, we must have $\sigma = \sigma(p) = \tau_2$.

If $p \mid A_n$ and $p \mid Y_n$, then $p \mid X_n$; also, by (51), (52) and (48), we must have, $p \mid R_n$ and $p \mid S_n$. Hence,

$$p \mid \bar{u}_n(r_1, q_1)\bar{v}_n(r_2, q_2) \quad \text{and} \quad p \mid \bar{u}_n(r_2, q_2)\bar{v}_n(r_1, q_1).$$

If $\tau_1 \mid n$, then $p \mid \bar{u}_n(r_1, q_1)$ and $p \nmid \bar{v}_n(r_1, q_1)$ by (57). Thus, $\tau_2 \mid n$ and $\rho = \rho(p) = \operatorname{lcm}[\tau_1, \tau_2]$. If $\tau_1 \nmid n$, then $p \mid \bar{v}_n(r_2, q_2)$. We must have $2 \mid \tau_2$ and $\tau_2/2 \mid n$. Also, $p \nmid \bar{u}_n(r_2, q_2)$ and $p \mid \bar{v}_n(r_1, q_1)$ and we must also have $2 \mid \tau_1$ and $\tau_1/2 \mid n$. In this case we put $\psi_i = \tau_i/2$ and let $2^{\lambda_i} \mid\mid \psi_i$ $(i = 1, 2)$. Since n/ψ_i $(i = 1, 2)$ must be odd, we must have $\lambda_1 = \lambda_2$. Thus, if $\lambda_1 \neq \lambda_2$, we have $\rho = \operatorname{lcm}[\tau_1, \tau_2]$. If $\lambda_1 = \lambda_2$, then $\rho = \operatorname{lcm}[\psi_1, \psi_2]$ and $\sigma \nmid \rho$.

We now have the following result.

Proposition 35. *Suppose $G = 1$, p is a prime such that $p \nmid 2P_1Q$ and $p \mid I$. If $2 \nmid \tau_1$ or $2 \nmid \tau_2$, then p must be monoapparitic in (A_n).*

Proof. In this case $\sigma = \tau_2$ and $\rho = \operatorname{lcm}[\tau_1, \tau_2]$. Thus, $\sigma \mid \rho$ and the result follows by Proposition 25. □

Before proceeding any further we will need some additional results concerning Lehmer sequences. It is easy to establish by induction that if $p \mid r$, then for n odd we have

$$\bar{v}_n(r, q) \equiv n(-q)^{\frac{n-1}{2}} \pmod{p}, \quad \bar{u}_n(r, q) \equiv (-q)^{\frac{n-1}{2}} \pmod{p}.$$

Thus, if $p \mid r$ and $2 \nmid n$, we have $p \mid \bar{v}_n(r, q) \Leftrightarrow p \mid n$. Also, if $2 \mid n$ and $p \mid r$, then $\bar{u}_n(r, q) \equiv n/2(-q)^{n/2} \pmod{p}$. Thus, if $p \mid r$ and $2 \mid n$, then $p \mid \bar{u}_n(r, q) \Leftrightarrow p \mid n/2$. Also, if $2 \mid n$ and $p \mid r$, then

$$u_n(r, q) \equiv n/2(-q)^{n/2} \pmod{p}.$$

Thus, if $p \mid r$ and $2 \mid n$, then $p \mid u_n(r, q) \Leftrightarrow p \mid n/2$. It follows that $(\bar{u}_n(r, q))$ is monoapparitic modulo p when $p \nmid 2q$.

It is well known ([4, §4]) that $p \mid \bar{u}_{p-\epsilon}$, where ϵ is the value of the Legendre symbol (rd/p). Thus, if $p \mid d$, then $p \mid \bar{u}_p$ and $\tau(p) = p$. Since p is odd, $\psi = \psi(p)$ does not exist in this case. If $p \nmid d$, then

$$p \mid \bar{v}_{\frac{p-\epsilon}{2}} \Leftrightarrow (q/p) = -1.$$

Hence, if $(q/p) = -1$, then ψ exists and $\psi \mid \frac{p-\epsilon}{2}$.

A special case of Proposition 35 occurs when $(q_1/p) = (q_2/p) = 1$ and $((d_1d_2)/p) = -1$. For in this case, $\tau_1 \mid \frac{p-\epsilon_1}{2}$, $\tau_2 \mid \frac{p-\epsilon_2}{2}$. Also, $\epsilon_1\epsilon_2 = ((r_1r_2d_1d_2)/p) = ((d_1d_2)/p) = -1$. It follows that if $2 \mid \tau_1$ and $2 \mid \tau_2$ we get $2 \mid \frac{p-\epsilon_1}{2}$ and $2 \mid \frac{p-\epsilon_2}{2}$, which means that $p \equiv 1 \pmod 4$ and $p \equiv -1 \pmod 4$, an impossibility.

If $G = 1$ and $S \neq 1$, it is shown in [12] than any odd fourth-order LDS (A_n) must have the form given in (54), i.e.,

$$A_n = v_n(\sqrt{r_1}, q_1)u_n(\sqrt{r_2}, q_2)/\sqrt{r_1}, \tag{62}$$

but it is not always the case that this (A_n) will actually be a divisibility sequence. For example, if $r_1 = r_2 = 7$ and $q_2 = 141002$, we see that (A_n) behaves like a divisibility sequence until we arrive at the 28^{th} term, where we discover that A_{14} is not a divisor of A_{28}. Indeed, as mentioned in [12], it is unlikely that and (A_n) exists when $G = 1$ and $S \neq 1$, but this has not yet been proved.

If in (54) we put $r = r_1$, $q = q_1$, $\mu_2 = \mu_1^s$, $\nu_2 = \nu_1^s$, then $r_2 = v_s(\sqrt{r}, q)^2 = r\bar{v}_s(r, q)^2$ and $q_2 = q^s$, where s is any fixed odd positive integer. For these values of r_1, r_2, q_1, q_2, (62) becomes

$$A_n = \bar{v}_n(r, q)\bar{u}_{ns}(r, q)/\bar{u}_s(r, q). \tag{63}$$

(This A_n is essentially the same function as that discovered by Koshkin [5] when $f(x) = (x + 1)(x^3 - 1)$ and $x = \alpha/\beta$, where $\alpha + \beta = \sqrt{r}$ and $\alpha\beta = q$.) It can be shown that this (A_n) is a fourth-order odd LDS with characteristic polynomial given by (2) with P_1, P_2, Q defined in (48); also, by using some identities that are satisfied by the Lehmer functions, we have $P_1 = r\bar{v}_s(r, q)$, $P_2 = q\bar{v}_{s-1}(r, q)\bar{v}_{s+1}(r, q)$, $Q = q^{s+1}$, $\Delta = (r - 4q)^2\bar{u}_s(r, q)^2$, $E = (qr(r - 4q)\bar{u}_{s-1}(r, q)\bar{u}_{s+1}(r, q))^2$, $A_2 = (r - 2q)\bar{v}_s(r, q)$ and $I = 0$. Notice that we have $S = 1$ here.

In the particular case of $s = 3$, we have $P_1 = r(r - 3q)$, $P_2 = q(r - 2q)(r^2 - 4rq + 2q^2)$, $Q = q^4$ and $A_2 = (r - 2q)(r - 3q)$, whereas for (U_n) we would have $A_2 = P_1 = r(r - 3q)$. If we put $r = 5$ and $q = 1$, we get $P_1 = 10$, $P_2 = 21$, $Q = 1$,

$$U_n = 0, 1, 10, 76, 540, 3751, 25840, 177451, 1217160, 8344876, 57202750, \\ 392089501, \ldots, (L_{4n} - L_{2n})/4,$$

and the odd sequence

$$0, 1, 6, 38, 252, 1705, 11628, 79547, 544824, 3733234, 25585230, 175356611, \ldots. \tag{64}$$

These sequences are listed as A215465 and A215466, respectively in the OEIS. The sequence (63) with different values for r and q will also yield the odd LDSs: A238536 $(r = 1, q = -1)$, A238537 $(r = 4, q = -1)$ and A238538 $(r = 9, q = 2)$.

The sequence (64) is an example of a LDS where 2 has the two ranks of appearance 2 and 3. Notice that $\bar{v}_3(1, 5) = 2$. Indeed, if $p \mid \bar{v}_s(r, q)$, then for (A_n) given by (63) we have $p \mid P_1$, $p \mid A_2$, $P_2 \equiv q^s(r - 4q) \pmod p$ and $Q = q^{s+1}$. We can now use (58) and (59) to show that

$$\bar{u}_{2n+1}(-P_2, Q) \equiv (-1)^n q^{ns}\bar{v}_{2n+1}(r, q) \pmod p.$$

Thus, if $p \mid \bar{v}_s(r,q)$, then $\psi(p)$ exists and by Proposition 21 there are two possible ranks of appearance of p in (A_n): 2 and ψ. Since $\psi \mid s$, we have $2 \nmid \psi$ and therefore the two ranks are distinct.

Now suppose $p \nmid \bar{v}_s(r,q)$ in (63). If $p \mid \bar{u}_s(r,q)$, then by (57), we have $p \mid d_2$ and therefore $\tau_2 = \tau_2(p) = p$. Since $2 \nmid \tau_2$, p must be monoapparitic in (A_n) by Proposition 35. Next, suppose that $p \nmid \bar{u}_s(r,q)$ and put $t = \gcd(s, \tau_1)$. It is easy to show that $\tau_2 = \tau_1/t$ in this case. Thus, if $t = 1$ or $2 \nmid \tau_1$, we have $\tau_2 \mid \tau_1$ and consequently p is monoapparitic in (A_n). If $t > 1$ and $2 \mid \tau_1$, then p has two distinct ranks of apparition in (A_n): $\omega_1 = \sigma = \tau_1/t$ and $\omega_2 = \rho = \tau_1/2$.

If we next select (A_n) in (63) with $s = 3$ and set $A_2 = r(r-2q)$, then it turns out that this (A_n) is also an odd fourth-order LDS with characteristic polynomial (2) and, as before, $P_1 = r(r-3q)$, $P_2 = q(r-2q)(r^2-4rq+2q^2)$, $Q = q^4$. Here, it can be shown that

$$A_n = \bar{u}_{2n}(r,q)u_n(\sqrt{r},q)^2 = \begin{cases} \bar{v}_n(r,q)\bar{u}_n^3(r,q), & \text{if } 2 \nmid n; \\ r\bar{v}_n(r,q)\bar{u}_n^3(r,q), & \text{if } 2 \mid n. \end{cases} \tag{65}$$

If we put $r = 5$, $q = 1$, we get the sequence

$$0, 1, 15, 128, 945, 6655, 46080, 317057, 2176335, 14925184, 102320625, \ldots, F_{4n} - 2F_{2n},$$

which appears as A127595 in the OEIS. This sequence is not monoapparitic modulo 5 as 5 has ranks 2 and 5 in (A_n). More generally, if $p \mid r$, then by Proposition 21, (A_n) in (65) has ranks of appearance $\omega_1 = 2$ and $\omega_2 = p$, but if $p \nmid r$, then p is monoapparitic in (A_n) with $\omega = \tau/2$ when $2 \mid \tau$ and $\omega = \tau$, otherwise.

If we put $r_1 = t^2$, $q_1 = q$, $r_2 = (t^2-2q)^2$, $q_2 = q^2$ and $A_2 = t^3$, we find that $\Delta = t^2(t^2-4q)^2$ and

$$A_n = u_n(t,q)^3. \tag{66}$$

The corresponding sequence (A_n) is clearly odd and a fourth-order LDS. For $t = 1$, $q = -1$, we get A056570 in the OEIS. Also, any prime p is clearly monoapparitic in (A_n). We should mention here that versions of (63), (65) and (66) were discovered, using a different approach, by Oosterhout [6].

We have seen, then, that there are infinitely many odd fourth-order LDSs when $G = S = 1$; are there any others apart from those mentioned here? Possibly, the answer to this question is yes, but no non-trivial examples are known to the authors, none were found during an extensive computer search and none appear in the OEIS.

7 Conclusion

Although we have completely solved the problem of when (A_n) can have either one or two ranks of appearance (modulo p), there are still three problems that remain outstanding:

1) Show that no (A_n) exists when $S \neq 1$, $G = 1$;

2) Show that no (A_n) exists when $S = G \neq 1$;

3) Find all possibilities of (A_n) when $S = G = 1$.

8 Acknowledgment

The authors are grateful to Christian Ballot, who carefully read an earlier version of this paper and made a number of helpful and insightful suggestions for improving it. We also wish to thank an anonymous referee, whose careful reading of the original submission of this paper resulted in a substantial improvement in its exposition.

References

[1] M. Abrate, S. Barbero, U. Cerutti, and N. Murru, Linear divisibility sequences and Salem numbers, *Pub. Math. Debrecen* **91** (2017), 247–259.

[2] S. Barbero, Generalized Vandermonde determinants and characterization of divisibility sequences, *J. Number Theory* **173** (2017), 371–377.

[3] J.-P. Bézivin, A. Pethö, and A. J. van der Poorten, A full characterization of divisibility sequences, *Amer. J. Math.* **112** (1990), 985–1001.

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

[5] Sergiy Koshkin, Non-classical linear divisibility sequences and cyclotomic polynomials, *Fibonacci Q.* **57** (2019), 68–80.

[6] A. D. Oosterhout, Characterization of divisibility sequences, Master's Thesis, Utrecht University, (2011).

[7] N. J. A. Sloane et al., The On-Line Encyclopedia of Integer Sequences, 2020. Available at https://oeis.org.

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

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

[10] H. C. Williams and R. K. Guy, Some fourth-order linear divisibility sequences, *Internat. J. Number Theory* **7** (2011), 1255–1277.

[11] H. C. Williams and R. K. Guy, Some monoapparitic fourth order divisibility sequences, *Integers* **12A** (2012), A17.

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

2010 *Mathematics Subject Classification*: Primary 11B37; Secondary 11Y11, 11B50.
Keywords: linear recurrence, Lucas function.

(Concerned with sequences A005013, A056570, A127595, A215465, A215466, A238536, A238537, and A238538.)

Received April 7 2021; revised versions received June 5 2021; June 22 2021. Published in *Journal of Integer Sequences*, July 1 2021.

Return to Journal of Integer Sequences home page.