#A17 INTEGERS 12A (2012): John Selfridge Memorial Issue

SOME MONOAPPARITIC FOURTH ORDER LINEAR DIVISIBILITY SEQUENCES

H. C. Williams

R. K. Guy

Received: 6/1/11, Accepted: 12/1/11, Published: 10/12/12

Abstract

A sequence of rational integers $\{A_n\}$ is said to be a divisibility sequence if $A_m \mid A_n$ whenever $m \mid n$. If the divisibility sequence $\{A_n\}$ also satisfies a linear recurrence relation of order k, it is said to be a linear divisibility sequence. The best known example of a linear divisibility sequence of order 2 is the Lucas sequence $\{u_n\}$, one particular instance of which is the famous Fibonacci sequence. In their extension of the Lucas functions to order 4 linear recursions, Williams and Guy showed that the order 4 analog $\{U_n\}$ of $\{u_n\}$ can have no more than two ranks of apparition for a given prime p and frequently has two such ranks, unlike the situation for $\{u_n\}$, which can only have one rank of apparition. In this paper we investigate the problem of finding those sequences $\{U_n\}$ which have only one rank of apparition for any prime p.

– In memory of John Selfridge, a close friend and collaborator for nearly half a century.

1. Introduction

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

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

When p, q are coprime integers, both $u_n(p,q)$ and $v_n(p,q)$ are integers for all $n \geq 0$ and are called the Lucas functions. The Lucas functions possess a number of properties (see Ribenboim [2, pp.53–83] or Williams [3, pp.69–95]) which make them particularly useful for primality testing. In particular, if $n \mid m$, then $u_n(p,q) \mid u_m(p,q)$; also, both $u_n(p,q)$ and $v_n(p,q)$ satisfy the second order linear recurrence

$$X_{n+1} = pX_n - qX_{n-1}$$

In general a linear recurring sequence of order k over the integers is a sequence $\{X_n\}$, where we have

$$X_{n+k} = A_1X_{n+k-1} + A_2X_{n+k-2} + A_3X_{n+k-3} + \cdots + A_kX_n$$

and $X_0, X_1, X_2, \dots, X_{k-1}, A_1, A_2, A_3, \dots, A_k$ are given fixed integers, with $A_k \neq 0$. Furthermore, if $X_m \mid X_n$ whenever $m \mid n$, then $\{X_n\}$ is said to be a kth order **divisibility sequence**. Thus, we see that the Lucas sequence $\{u_n(p,q)\}$ is a second order divisibility sequence. This sequence also has the property that $(u_n, u_m) = |u_g|$ where $g = (m,n)$ and we use the notation (a,b) with $a, b \in \mathbb{Z}$ to denote the greatest common divisor of a and b.

If a divisibility sequence $\{A_n\}$ is such that $(A_n, A_m) = |A_g|$, where $g = (m,n)$, we say that $\{A_n\}$ is a **strong** divisibility sequence.

In his investigation of the problem of primality testing, Lehmer [1] introduced the functions $\bar{u}_n(r,q)$, $\bar{v}_n(r,q)$ where r, q are coprime integers. These are defined by

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

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

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

$$X_{n+4} = (r - 2q)X_{n+2} - q^2 X_n$$

Furthermore, $\{\bar{u}_n(r,q)\}$ is a strong divisibility sequence. Further properties of the Lehmer functions can be found in [1].

In their study of a fourth order analog of the Lucas functions, Williams & Guy [4] defined $U_n = U_n(P_1, P_2, Q)$, $V_n = V_n(P_1, P_2, Q)$, where P_1, P_2, Q are integers, $(P_1, P_2, Q) = 1$, and

$$U_n = \frac{\alpha_1^n + \beta_1^n - \alpha_2^n - \beta_2^n}{\alpha_1 + \beta_1 - \alpha_2 - \beta_2} \qquad V_n = \alpha_1^n + \beta_1^n + \alpha_2^n + \beta_2^n$$

Here $\alpha_1\beta_1 = \alpha_2\beta_2 = Q$, $\alpha_1 + \beta_1 = \rho_1$, $\alpha_2 + \beta_2 = \rho_2$ and ρ_1, ρ_2 are the zeroes of $f(x) = x^2 - P_1 x + P_2$. Note that α_1, β_1, α_2, β_2 are the zeroes of

$$F(x) = x^4 - P_1 x^3 + (P_2 + 2Q)x^2 - QP_1 x + Q^2$$

Thus, U_n and V_n satisfy the fourth order linear recurrence

$$X_{n+4} = P_1 X_{n+3} - (P_2 + 2Q)X_{n+2} + P_1 Q X_{n+1} - Q^2 X_n$$

Also, the discriminant D of $F(x)$ is given by

$$D = E\Delta^2 Q^2$$

where $\Delta = P_1^2 - 4P_2$ and $E = (P_2 + 4Q)^2 - 4QP_1^2$. We will assume throughout this work that $D \neq 0$ so that the zeroes of $F(x)$ are distinct.

We notice that $U_{-1} = 1/Q$, $U_0 = 0$, $U_1 = 1$, $U_2 = P_1$, $U_3 = P_1^2 - P_2 - 3Q$. If we change the sign of P_1 and consider the sequence $\{U_n^*\}$ where $U_{-1}^* = 1/Q$, $U_0^* = 0$, $U_1^* = 1$, $U_2^* = -P_1$,

$$U_{n+4}^* = (-P_1)U_{n+3}^* - (P_2 + 2Q)U_{n+2}^* + (-P_1)QU_{n+1}^* - Q^2 X_n$$

it is easy to establish by induction that

$$U_n^* = U_n(-P_1, P_2, Q) = (-1)^{n-1} U_n(P_1, P_2, Q)$$

Thus, by changing the sign of P_1 we only change the sign of U_{2n}.

It is possible to show that just about every important property of the Lucas functions has an exact analog in the theory of the U_n and V_n functions. However, there is one result for U_n that does not have an analog in this theory: the $\{U_n\}$ sequence is not in general a strong divisibility sequence. For example, take $P_1 = 1$, $P_2 = -7$, $Q = 1$. In this case we have $U_6 = 95$, $U_{20} = 217172736$ and $(U_6, U_{20}) = 19$, whereas $U_{(6,20)} = U_2 = 1$. It turns out that the least positive integer n for which $19 \mid U_n$ is $n = 6$, but even though $19 \mid U_{20}$, we do not have $6 \mid 20$. In the next section we investigate this phenomenon more closely.

2. Laws of Apparition

We begin this section with a definition.

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

In [4] it is shown that there can be at most two ranks of apparition of a prime p in $\{U_n\}$. Indeed, if $p \nmid \Delta Q$; $\mathbb{K}$ denotes the splitting field of $F(x)$ in $\mathbb{F}[x]$; α_1, β_1, α_2, β_2 are the zeroes of $F(x)$ in $\mathbb{K}$; and p has two ranks of apparition, ω_1 and ω_2 in $\{U_n\}$, then ω_1 is the least integer for which $\alpha_1^{\omega_1} = \alpha_2^{\omega_1}$ in $\mathbb{K}$ and ω_2 is the least integer for which $(\alpha_1\alpha_2)^{\omega_2} = Q^{\omega_2}$ in $\mathbb{K}$. It is this possibility, that a prime p can have two ranks of apparition in $\{U_n\}$ that prevents $\{U_n\}$ from being a strong divisibility sequence.

Proposition 2.1. If p is any prime that has two ranks of apparition in $\{U_n\}$, then $\{U_n\}$ cannot be a strong divisibility sequence.

Proof. Let p have two ranks of apparition, ω_1 and ω_2 in $\{U_n\}$, where $\omega_1 < \omega_2$ and $\omega_1 \nmid \omega_2$. Clearly $p \mid (U_{\omega_1}, U_{\omega_2})$. If $g = (\omega_1, \omega_2)$, we see that $0 < g < \omega_1$. If $(U_{\omega_1}, U_{\omega_2}) = |U_g|$, then $p \mid U_g$, contrary to the definition of ω_1. □

Definition. The divisibility sequence $\{U_n\}$ is said to be **monoapparitic** if there is only one rank of apparition for each prime which divides a term of the sequence.

We have seen in Proposition 2.1 that a necessary condition that $\{U_n\}$ be a strong divisibility sequence is that $\{U_n\}$ be monoapparitic. However, this condition is not sufficient. As we shall see below, the sequence given by $P_1 = -5$, $P_2 = -14$, $Q = 16$ is monoapparitic, but $11^2 \mid U_{12}$ and $11^2 \mid U_{44}$. Now $4 = (12, 44)$ and $U_4 = 55$ so that $|U_4| \neq (U_{12}, U_{44})$. In this paper we will attempt to determine monoapparitic $\{U_n\}$. To assist us in this investigation we list a number of results from [4].

1. If $p = 2$, then p has two ranks of apparition if and only if $2 \mid P_1$ and $2 \nmid P_2Q$.

2. If p is odd and $p \mid Q$, then p has only one rank of apparition in $\{U_n\}$.

3. If p is odd and $p \nmid Q$, $p \mid \Delta$ and $p \nmid E$, then p has two ranks of apparition in $\{U_n\}$.

4. If p is odd, $p \nmid Q$, $p \mid \Delta$ and $p \mid E$, then p has only one rank of apparition in $\{U_n\}$.

5. If p is odd, $p \nmid Q$, $p \nmid \Delta$ and $p \mid E$, then p can have two ranks of apparition in $\{U_n\}$.

We next consider the case where $p \nmid 2Q\Delta E$.

6. If $\left(\frac{E}{p}\right) = -1$, then p has only one rank of apparition in $\{U_n\}$.

7. If $\left(\frac{E}{p}\right) = 1$, and $\left(\frac{\Delta}{p}\right) = -1$, then p has two ranks of apparition in $\{U_n\}$ when $p \nmid P_1$.

In this case we see that if $p \nmid P_1$, we must have $\left(\frac{\Delta}{p}\right) = 1$ in order for p to have a single rank of apparition in $\{U_n\}$. Indeed, as there must exist an infinitude of primes p such that $p \nmid P_1$ and $\left(\frac{E}{p}\right) = 1$, we see that $\left(\frac{\Delta}{p}\right) = 1$ for all of these primes if $\{U_n\}$ is to be monoapparitic. In the next section we will show that if $\{U_n\}$ is monoapparitic and $E = GU^2$, $\Delta = SV^2$, where G, S are squarefree, then we must have $G = S$ or $S = 1$.

3. Types of Monoapparitic $\{U_n\}$

In order to establish the main result of this section we require several preliminary results.

Lemma 3.1. Let K (> 1) be a squarefree integer and let the values of η, λ be preselected from the set $\{1, -1\}$. There exists an integer r such that $r \equiv \lambda \pmod 4$ and such that if p is any prime satisfying $p \equiv r \pmod{4K}$, then $\left(\frac{K}{p}\right) = \eta$.

Proof. We consider two cases.

`Case 1.` $2 \nmid K$. Let q be any prime divisor of K. There exists an integer s such that

$$\left(\frac{s}{q}\right) = (-1)^{\frac{K-1}{2}\frac{\lambda-1}{2}}\eta$$

We may now use the Chinese remainder theorem (CRT) to find a value of r such that

$$r \equiv s \pmod{q}, \quad r \equiv 1 \pmod{K/q}, \quad \text{and} \quad r \equiv \lambda \pmod{4}$$

because q, K/q and 4 are coprime in pairs.

Now if p is prime,

$$\left(\frac{K}{p}\right) = (-1)^{\frac{p-1}{2}\frac{K-1}{2}}\left(\frac{p}{K}\right) = (-1)^{\frac{p-1}{2}\frac{K-1}{2}}\left(\frac{p}{q}\right)\left(\frac{p}{K/q}\right)$$

If $p \equiv r \pmod{4K}$, then $p \equiv \lambda \pmod{4}$, $p \equiv s \pmod{q}$, $p \equiv 1 \pmod{K/q}$. Hence

$$\left(\frac{K}{p}\right) = (-1)^{\frac{\lambda-1}{2}\frac{K-1}{2}}\left(\frac{s}{q}\right) = \eta$$

`Case 2.` $2 \mid K$. In this case $K = 2M$ and M is odd. If p is a prime,

$$\left(\frac{K}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{M}{p}\right)$$

If $M = 1$, put $r = 3$ if $\eta = \lambda = -1$; put $r = 7$ if $\eta = 1$, $\lambda = -1$; put $r = 5$ if $\eta = -1$, $\lambda = 1$; and put $r = 1$ if $\eta = \lambda = 1$. Thus, if $p \equiv r \pmod{8}$ $(8 = 4K)$, we get

$$\left(\frac{K}{p}\right) = \left(\frac{2}{p}\right) = \eta$$

If $M > 1$, then by the first case of the lemma there exists some $k \equiv \lambda \pmod{4}$ such that if a prime $p \equiv k \pmod{4M}$, then $\left(\frac{M}{p}\right) = \eta$. Put $t \equiv 2^{-1}\frac{k-\lambda}{4} \pmod{M}$ and $r = \lambda + 8t$. If $p \equiv r \pmod{8M}$ $(8M = 4K)$, then

$$p \equiv \lambda \pmod{8} \Rightarrow \left(\frac{2}{p}\right) = 1$$

But $r \equiv \lambda + 8\left(2^{-1}\frac{k-\lambda}{4}\right) \equiv k \pmod{8M}$; thus, $\left(\frac{K}{p}\right) = \left(\frac{M}{p}\right) = \eta$ □

Corollary 3.1.1. Let K be a squarefree integer with $|K| > 1$ and let the values of η and λ be preselected from the set $\{1, -1\}$. There exists an integer r with $r \equiv \lambda \pmod{4}$ such that if p is any prime satisfying $p \equiv r \pmod{4|K|}$, then $\left(\frac{K}{p}\right) = \eta$.

Proof. We have

$$\left(\frac{K}{p}\right) = \lambda\left(\frac{|K|}{p}\right) \quad (|K| > 1)$$

By the lemma, there exists some $r \equiv \lambda \pmod{4K}$ such that if $p \equiv r \pmod{4K}$, then $\left(\frac{|K|}{p}\right) = \lambda\eta \Rightarrow \left(\frac{K}{p}\right) = \eta$. □

Lemma 3.2. Given k positive integers $A_1, A_2, \ldots, A_k$ which are coprime in pairs and integers $r_1, r_2, \ldots, r_k$ such that $r_i \equiv r_j \pmod 4$ $(1 \le i, j \le k)$, there exists an integer r such that $r \equiv r_i \pmod{4A_i}$ $(i = 1, 2, \ldots, k)$.

Proof. Since $r_1 \equiv r_2 \equiv \cdots \equiv r_k \pmod 4$, we may assume that $r_i \equiv \lambda \pmod 4$ for some fixed λ $(0 \le \lambda < 4)$. By the CRT we can find some s such that

$$s \equiv (r_i - \lambda)/4 \pmod{A_i} \quad (i = 1, 2, \ldots, k)$$

Putting $r = \lambda + 4s$ we get the desired result. □

We are now able to prove the following theorem. We use $[a, b]$ to denote the least common multiple of the integers a and b.

Theorem 3.3. Let K, L be squarefree integers such that $|K| \neq |L|$ and $|K|$, $|L| > 1$. Let the values of η_1, η_2 and λ be preselected from the set $\{1, -1\}$. There exists an integer r such that $r \equiv \lambda \pmod 4$ and if p is any prime such that

$$p \equiv r \pmod{[4|K|, 4|L|]}$$

then $\left(\frac{K}{p}\right) = \eta_1$, $\left(\frac{L}{p}\right) = \eta_2$.

Proof. Put $D = (K, L)$; we have $(K/D, D) = (L/D, D) = (K/D, L/D) = 1$. We may assume with no loss of generality that $|K| > |L|$. As in the proof of Lemma 3.1, we distinguish two cases.

`Case 1`. $|L|/D > 1$. By Corollary 3.1.1 we know that there exist integers r_1 and r_2 such that $r_1 \equiv r_2 \equiv \lambda \pmod 4$ and if p is any prime satisfying

$$p \equiv r_1 \pmod{4|K|/D}, \qquad p \equiv r_2 \pmod{4|L|/D}$$

then $\left(\frac{K/D}{p}\right) = \eta_1$, $\left(\frac{L/D}{p}\right) = \eta_2$. Also, there exists an integer r_3 such that $r_3 \equiv \lambda \pmod 4$ and if p is any prime satisfying $p \equiv r_3 \pmod{4D}$, then $\left(\frac{D}{p}\right) = 1$.

By Lemma 3.2 there must exist some r such that

$$\begin{aligned} r &\equiv \lambda \pmod 4 \\ r &\equiv r_1 \pmod{4|K|/D} \\ r &\equiv r_2 \pmod{4|L|/D} \\ r &\equiv r_3 \pmod{4D} \end{aligned}$$

If $p \equiv r \pmod{[4|K|, 4|L|]}$, then

$$\left(\frac{K}{p}\right) = \left(\frac{K/D}{p}\right)\left(\frac{D}{p}\right) = \eta_1, \qquad \left(\frac{L}{p}\right) = \left(\frac{L/D}{p}\right)\left(\frac{D}{p}\right) = \eta_2$$

Case 2. $|L|/D = 1$. In this case, by Lemma 3.1, there exists an integer r_1 such that $r_1 \equiv \lambda \pmod 4$ and if p is any prime satisfying $p \equiv r_1 \pmod{4|K|/D}$, then

$$\left(\frac{K/D}{p}\right) = \eta_1\eta_2\lambda.$$

Also, since $D > 1$, there exists an integer $r_3 \equiv \lambda \pmod 4$ such that if $p \equiv r_3 \pmod 4$, then $\left(\frac{D}{p}\right) = \eta_2\lambda$. By Lemma 3.2, we can find $r \equiv \lambda \pmod 4$ such that

$$\begin{aligned} r &\equiv r_1 \pmod{4|K|/D} \\ r &\equiv r_3 \pmod{4D} \end{aligned}$$

If p is any prime satisfying $p \equiv r \pmod{[4|K|, 4|L|]}$ then

$$p \equiv r \pmod{4|K|}, \qquad p \equiv r_1 \pmod{4|K|/D}, \qquad p \equiv r_3 \pmod{4D}.$$

Hence

$$\left(\frac{K}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{K/D}{p}\right) = \eta_2\lambda\eta_1\eta_2\lambda = \eta_1, \qquad \left(\frac{L}{p}\right) = \lambda\left(\frac{D}{p}\right) = \eta_2 \qquad \square$$

We are now able to prove the result mentioned at the end of **§2.**

Theorem 3.4. Let $\Delta = SV^2$ and $E = GU^2$, where S, G, U, V are integers and S and G are squarefree. If $\{U_n\}$ is monoapparitic, then $S = G$ or $S = 1$.

Proof. Put $\lambda = 1$, $\eta_1 = -1$, $\eta_2 = 1$, $K = S$, $L = G$. We first suppose that $|G| > 1$. If $|S| \neq |G|$ and $|S| \neq 1$, then by Theorem 3.3 there exists an integer $r \equiv \lambda \pmod 4$ such that if p is an prime satisfying $p \equiv \lambda \pmod{[4|S|, 4|G|]}$, then $\left(\frac{S}{p}\right) = \eta_1 = -1$, $\left(\frac{G}{p}\right) = \eta_2 = 1$. Then, by Dirichlet's theorem, we know that there exists an infinitude of primes p such that $\left(\frac{E}{p}\right) = 1$, $\left(\frac{\Delta}{p}\right) = -1$. But by Remark 7 in **§2**, we know that p must have two ranks in $\{U_n\}$. Thus, for $\{U_n\}$ to be monoapparitic, we must have $|S| = |G|$ or $|S| = 1$.

We now consider the case $S = -G$. By Lemma 3.1 we know that there exists an infinitude of primes $p \equiv -1 \pmod 4$ such that

$$\left(\frac{S}{p}\right) = -1 \Longrightarrow \left(\frac{G}{p}\right) = \left(\frac{-S}{p}\right) = 1 \Longrightarrow \left(\frac{\Delta}{p}\right) = -1, \left(\frac{E}{p}\right) = 1.$$

As this is not possible for a monoapparitic $\{U_n\}$, we must have $S = G$.

We next consider the case $|S| \neq |G|$ and $|S| = 1$. If we put $\lambda = -1$, $K = G$, $\eta = 1$ in Lemma 3.1, we see that there must exist an infinitude of primes p such that $p \equiv -1 \pmod 4$ and $\left(\frac{E}{p}\right) = 1$. If $S = -1$, then $\left(\frac{\Delta}{p}\right) = \left(\frac{-1}{p}\right) = -1$, which is not possible if $\{U_n\}$ is monoapparitic. Hence $S = 1$.

Next, if $G = 1$, then $\left(\frac{\Delta}{p}\right) = 1$ for all primes p, which means that $S = 1$ implies $S = G$.

Finally, if $G = -1$, we put $\lambda = 1$, $K = S$, $\eta = -1$. If $|K| > 1$ we know from Corollary 3.1.1 that there exists an infinitude of primes p such that $\left(\frac{\Delta}{p}\right) = \left(\frac{S}{p}\right) = -1$. Since $\left(\frac{E}{p}\right) = \left(\frac{G}{p}\right) = \left(\frac{-1}{p}\right) = 1$, $\{U_n\}$ cannot be monoapparitic.

Thus, $|S| = 1$. If $S = -1$, then $S = G$; otherwise $S = 1$. $\square$

It follows that if $\{U_n\}$ is to be monoapparitic we must have three possible cases.

1. E is a square and Δ is a square.
2. E is a not square and Δ is a square.
3. E and Δ are not squares, but $E\Delta$ is a square.

In the sections that follow we will deal with each of these cases.

4. The Case of E a Square

In this section we will investigate whether there exist any monoapparitic $\{U_n\}$ when E is a perfect square. We will need the following result.

Theorem 4.1. If $E = U^2$, then there must exist integers r_1, r_2, q_1, q_2 satisfying $r_1 > 0$, $r_2 > 0$, r_1r_2 a perfect square, $(r_1, q_1) = (r_2, q_2) = 1$ such that

$$P_1^2 = r_1r_2, \quad P_2 = q_1r_2 + q_2r_1 - 4q_1q_2, \quad Q = q_1q_2$$

Proof. Putting $W = P_2 + 4Q$, $T = P_1$, we get $W^2 - U^2 = 4QT^2$. Put $d = (U, T)$, $d' = (W, T)$. We have $d^2 \mid W^2$, and hence $d \mid W$ so that $d \mid d'$. Also, $d'^2 \mid U^2$ implies $d' \mid U$, and therefore $d' \mid d$. Hence $d = d'$ or $(U, T) = (W, T)$. Put

$$U' = U/d, \quad T' = T/d, \quad W' = W/d$$

We get

$$\left(\frac{W' - U'}{2}\right)\left(\frac{W' + U'}{2}\right) = QT'^2$$

Put $G = \left(\frac{W'-U'}{2}, \frac{W'+U'}{2}\right)$. Since $G \mid W'$ and $G \mid U'$ we must have $(G, T') = 1$; Hence $G^2 \mid Q$. It follows that

$$\left(\frac{W' - U'}{2G}\right)\left(\frac{W' + U'}{2G}\right) = \left(\frac{Q}{G^2}\right)T'^2$$

Since $\left(\frac{W'-U'}{2G}, \frac{W'+U'}{2G}\right) = 1$ we must have

$$\frac{W'+U'}{2G} = Q_1' R_2^2, \quad \left(\frac{W'-U'}{2G}\right) = Q_2' R_1^2,$$

where $(Q_1' R_2, Q_2' R_1) = 1$, $Q_1' Q_2' = Q/G^2$ and $T' = R_1 R_2$. If we put $q_1 = GQ_1'$, $q_2 = GQ_2'$, $r_2 = dR_2^2$, $r_1 = dR_1^2$, we get $P_1^2 = T^2 = r_1 r_2$, $Q = q_1 q_2$, $W = q_1 r_2 + q_2 r_1$, $P_2 = q_1 r_2 + q_2 r_1 - 4q_1 q_2$. Also, since $d > 0$, we must have $r_1,\ r_2 > 0$. If p is any prime which divides (r_1, q_1) or (r_2, q_2), then $p \mid P_1$, $p \mid Q$, $p \mid P_2$, which is not possible. Thus $(r_1, q_1) = (r_2, q_2) = 1$. □

Corollary 4.1.1. If E is a perfect square, then $|U_n| = |u_n(\sqrt{r_1}, q_1) u_n(\sqrt{r_2}, q_2)|$, where r_1, q_1, r_2, q_2 are as in Theorem 4.1.

Proof. Define $\mu_1,\ \nu_1,\ \mu_2,\ \nu_2$, by

$$\mu_1 + \nu_1 = \sqrt{r_1}, \qquad \mu_1 \nu_1 = q_1, \qquad \mu_2 + \nu_2 = \sqrt{r_2}, \qquad \mu_2 \nu_2 = q_2$$

If we put $\alpha_1 = \mu_1 \mu_2,\ \beta_1 = \nu_1 \nu_2,\ \alpha_2 = \nu_1 \mu_2,\ \beta_2 = \mu_1 \nu_2$, we have

$$\alpha_1 \beta_1 = \alpha_2 \beta_2 = q_1 q_2 = Q.$$

Also, if $\rho_1 = \alpha_1 + \beta_1,\ \rho_2 = \alpha_2 + \beta_2$, then

$$\begin{aligned}
\rho_1 + \rho_2 &= \mu_1\mu_2 + \nu_1\nu_2 + \nu_1\mu_2 + \mu_1\nu_2 = (\mu_1 + \nu_1)(\mu_2 + \nu_2) = \sqrt{r_1 r_2} \ = \ \pm P_1 \\
\rho_1 \rho_2 &= (\mu_1\mu_2 + \nu_1\nu_2)(\nu_1\mu_2 + \mu_1\nu_2) \\
&= q_1(\mu_2^2 + \nu_2^2) + q_2(\mu_1^2 + \nu_1^2) \\
&= q_1 r_2 + q_2 r_1 - 4q_1 q_2 \quad = \quad P_2
\end{aligned}$$

Thus, if $\rho_1 + \rho_2 = P_1$, then ρ_1, ρ_2 are the zeroes of $f(x)$ and

$$U_n = \frac{\alpha_1^n + \beta_1^n - \alpha_2^n - \beta_2^n}{\alpha_1 + \beta_1 - \alpha_2 - \beta_2} = \left(\frac{\mu_1^n - \nu_1^n}{\mu_1 - \nu_1}\right)\left(\frac{\mu_2^n - \nu_2^n}{\mu_2 - \nu_2}\right) = u_n(\sqrt{r_1}, q_1) u_n(\sqrt{r_2}, q_2).$$

If $\rho_1 + \rho_2 = -P_1$, then, since we have seen that

$$U_n(-P_1, P_2, Q) = (-1)^{n-1} U_n(P_1, P_2, Q),$$

we get our result. □

Now suppose we define $\mu_2 = \mu_1^s,\ \nu_2 = \nu_1^s$, where $\mu_1 + \nu_1 = \sqrt{r},\ \mu_1\nu_1 = q$, $(r, q) = 1$. In this case we get

$$U_n = \frac{u_n u_{sn}}{u_s} \tag{4.1}$$

where $u_m = u_m(\sqrt{r}, q)$. Here we have $\alpha_1 = \mu_1^{s+1}$, $\beta_1 = \nu_1^{s+1}$, $\alpha_2 = q\mu_1^{s-1}$, $\beta_2 = q\nu_1^{s-1}$, $\rho_1 = v_{s+1}$, $\rho_2 = qv_{s-1}$, $Q = q^{s+1}$, where $v_m = v_m(\sqrt{r}, q)$. Note that we can verify from the formulas for u_m and v_m in terms of μ_1 and ν_1 that

$$rv_m^2 - 4qv_{m+1}v_{m-1} = (r-4q)^2u_m^2 \quad \text{and} \quad v_m^2 - (r-4q)u_m^2 = 4q^m.$$

We find that

$$P_1 = \sqrt{r}v_s, \quad P_2 = qv_{s-1}v_{s+1}, \quad \Delta = (r-4q)^2u_s^2$$
$$\text{and} \quad E = (\rho_1^2 - 4Q)(\rho_2^2 - 4Q) = q^2(r-4q)^2u_{s-1}^2u_{s+1}^2$$

Now E here is always a perfect integer square.

In the case where s is odd, we always have Δ an integer square, but if s is even, then $u_s = \sqrt{r}\bar{u}_s$ where $\bar{u}_s$ is an integer, hence for Δ to be a square we need r to be a perfect square. Under these conditions we have $u_n \in \mathbb{Z}$ $(n \geq 0)$ and the following result.

Theorem 4.2. If p is a prime and $p \nmid 2Q\Delta$, then p has only one rank of apparition in $\{U_n\}$, where U_n is given by (4.1).

Proof. The proof of the result is similar to, but easier than, the proof of Theorem 5.1 below. Thus we refer the reader to Theorem 5.1. □

We know that if $p \mid Q$, then p has only one rank of apparition in the sequence $\{U_n\}$ as defined by (4.1). Suppose $p \nmid Q$. If p is odd and $p \mid \Delta$, then $p \nmid u_s$, implying $p \mid E$ and hence p has only one rank of apparition in $\{U_n\}$. However, if $p \mid u_s$, then since $u_s^2 - u_{s-1}u_{s+1} = q^{s-1}$ we see that $p \nmid u_{s-1}u_{s+1}$ when $p \nmid q$. Thus, if $p \mid u_s$, then in order for p to have only one rank of apparition in $\{U_n\}$, we must have $p \mid r - 4q$. It follows that if all the distinct primes which divide u_s also divide $r - 4q$, then $\{U_n\}$, where U_n is given by (4.1), is monoapparitic. Unfortunately, this is difficult to ensure on selecting an r, q pair. However, we can produce the following result.

Theorem 4.3. Suppose p is a prime, $p \mid s$ and $|u_s| = |\bar{u}_s| = p^k$ $(k \geq 0)$. If ω is the least positive integer n such that $p \mid U_n$, where U_n is given by (4.1), then if $p \mid U_m$, we must have $\omega \mid m$.

Proof. Let λ be the rank of apparition of $\{\bar{u}_n\}$ modulo p. We must have $p \mid \bar{u}_s$ and $p \mid s$; also,

$$\lambda \mid s \implies \bar{u}_\lambda \mid \bar{u}_s \implies \lambda = p^\kappa \ (\kappa \leq k).$$

However, by the Law of Apparition for Lehmer functions [1, Theorem 1.7], we must have $\lambda \mid p$ or $\lambda \mid p \pm 1$. Since $(p, p \pm 1) = 1$, we can only have $\lambda = p$. Also, since $p \mid U_\lambda$, we must have $\omega \leq \lambda$. If $p \mid \bar{u}_\omega$, then $\lambda \mid \omega$ implies $\omega = \lambda = p$. If $p \mid \bar{u}_m$, then $\lambda \mid m$ implies $\omega \mid m$. Suppose $p \mid \bar{u}_\omega$ and $p \nmid \bar{u}_m$. In this case, since $p \mid U_m$, we have $p \mid \bar{u}_{sm}/\bar{u}_s$. It is a simple matter, using the methods of, say, [3, p.86] to establish that

$$\left(\frac{\bar{u}_{sm}}{\bar{u}_s}, \bar{u}_s\right) \Bigg| \ m.$$

Since $p \mid \bar{u}_s$, we must have $p \mid m$ so that $\omega \mid m$. If $p \nmid \bar{u}_\omega$, then $p \mid \bar{u}_{sw}/\bar{u}_s$. Therefore $p \mid \omega$ and hence $\lambda \mid \omega$ so that $\omega = \lambda$ which implies $p \mid \bar{u}_\omega$, a contradiction. $\square$

Now suppose that u_s is given as in Theorem 4.3. Then the sequence $\{U_n\}$ as given in (4.1) is monoapparitic if 2 has at most one rank of apparition in $\{U_n\}$.

We note that, since $\sqrt{r} = \alpha + \beta$, we have $r \mid v_{2k-1}v_{2k+1}$ and by induction $v_{2k} \equiv r \pmod 2$. If $2 \mid q$, then $2 \mid Q$ and therefore 2 has at most one rank of apparition in $\{U_n\}$. If $2 \mid r$, then $2 \mid P_1 = U_2$ implies that 2 has at most one rank of apparition in $\{U_n\}$. We now suppose that $2 \nmid r$. Since, when $2 \mid s$, $v_2 \equiv 1 \pmod 2$, we see that $2 \nmid P_1$; hence 2 can have at most one rank of apparition in $\{U_n\}$. If s is odd, then $|u_s| = p^k$, where $p \mid s$, means that $2 \nmid U_s$. Since $v_s^2 \equiv ru_s^2 \pmod 4$, we have $2 \nmid v_s$ so that $2 \nmid P_1$. It follows that $\{U_n\}$, given by (4.1), is always monoapparitic when $|u_s| = p^k$, where p is some prime divisor of s.

Example 1. Consider the case $s = 2$. Here r must be a perfect square, say $r = t^2$. We have $U_n = u_n^2(t,q)v_n(t,q)/t$. Now $u_s = u_2 = t$. Thus, if $t = \pm 2^k$ with $k \geq 0$, then $\{U_n\}$ is monoapparitic. Here $P_1 = t(t^2 - 2q)$, $P_2 = qt^2(t^2 - 3q)$, $Q = q^3$.

Example 2. We next consider the case $s = 3$. Here $u_s = u_3 = r - q$ and

$$U_n = u_n(\sqrt{r}, q)u_{3n}(\sqrt{r}, q)/u_3(\sqrt{r}, q).$$

If $r - q = \pm 3^k$ with $k \geq 0$, then $\{U_n\}$ is monoapparitic. Here $P_1 = r(r - 3q)$, $P_2 = r^3q - 6r^2q^2 + 10rq^3 - 4q^4 = q(r - 2q)(r^2 - 4rq + 2q^2)$, $Q = q^4$. If we put $r = 4$, $q = 1$, we get $P_1 = 4$, $P_2 = 4$, $Q = 1$ and $U_n = n^2$ which is clearly monoapparitic and strong.

Indeed, we have shown that if E is a perfect square, there exist infinitely many $\{U_n\}$ which are monoapparitic.

5. Another Monoapparitic $\{U_n\}$ When E Is a Square

In this section we will produce another set of sequences $\{U_n\}$ that are monoapparitic when E is a perfect square. As before we define μ_1 and ν_1 by $\mu_1 + \nu_1 = \sqrt{r}$, $\mu_1\nu_1 = q$, where r, q are coprime integers. We now put $\mu_2 = i\mu_1^s$, $\nu_2 = -i\nu_1^s$, where $i^2 + 1 = 0$. Here

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

where $\alpha_1 = i\mu_1^{s+1}$, $\beta_1 = -i\nu_1^{s+1}$, $\alpha_2 = iq\mu_1^{s-1}$, $\beta_2 = -iq\nu_1^{s-1}$. We denote by u_n and v_n the functions $u_n(\sqrt{r}, q)$ and $v_n(\sqrt{r}, q)$ respectively. We get

$$\begin{aligned}
\rho_1 &= \mu_1\mu_2 + \nu_1\nu_2 = i(\mu_1^{s+1} - \nu_1^{s+1}) = i(\mu_1 - \nu_1)u_{s+1} \\
\rho_2 &= \nu_1\mu_2 + \mu_1\nu_2 = qi(\mu_1 - \nu_1)u_{s-1} \\
P_1 &= \rho_1 + \rho_2 = i(\mu_1 - \nu_1)(u_{s+1} + qu_{s-1}) = i(\mu_1 - \nu_1)\sqrt{r}u_s \\
P_2 &= \rho_1\rho_2 = -q(\mu_1 - \nu_1)^2 u_{s+1}u_{s-1} = q(4q - r)u_{s+1}u_{s-1} \\
Q &= \alpha_1\beta_1 = q^{s+1}
\end{aligned}$$

We find that

$$\begin{aligned}
\rho_1^2 - 4Q &= -(r - 4q)u_{s+1}^2 - 4q^{s+1} = -v_{s+1}^2 \\
\rho_2^2 - 4Q &= -q^2(r - 4q)u_{s-1}^2 - 4q^{s+1} = -q^2v_{s-1}^2
\end{aligned}$$

Thus $$E = (\rho_1^2 - 4Q)(\rho_2^2 - 4Q) = q^2v_{s-1}^2v_{s+1}^2$$

Also $$\begin{aligned}\Delta = P_1^2 - 4P_2 &= -(\mu_1 - \nu_1)^2ru_s^2 - 4q(4q - r)u_{s+1}u_{s-1} \\ &= (4q - r)(ru_s^2 - 4qu_{s+1}u_{s-1})\end{aligned}$$

It is easy to verify from the formulas for u_n and v_n in terms of μ_1 and ν_1 that

$$ru_n^2 - 4qu_{n+1}u_{n-1} = v_n^2$$

Hence $\Delta = (4q - r)v_s^2$.

Since E is a perfect square, in order for $\{U_n\}$ to be monoapparitic, Δ must also be a perfect square; therefore we put $t^2 = 4q - r$ and find that $P_1 = -t\sqrt{r}u_s$. Since P_1 must be a rational integer, we see that if $2 \nmid s$ we must have r a perfect square. We assume that this condition is satisfied in what follows. We can now represent $\{U_n\}$ by

$$U_n = \begin{cases} (-1)^{n/2}tu_nu_{sn}/v_s & \text{when } 2 \mid n \\ (-1)^{(n-1)/2}u_nv_{sn}/v_s & \text{when } 2 \nmid n \end{cases} \tag{5.1}$$

With no loss of generality we may write $\mu_1 = (\sqrt{r} + it)/2$, $\nu_1 = (\sqrt{r} - it)/2$. Let p be any odd prime such that $p \nmid \Delta Q$ and let $\mathbb{K}$ be the splitting field of $F(x)$ in $\mathbb{F}_p[x]$. By results in [4] we know that since both E and Δ are perfect squares, $\mathbb{K} = \mathbb{F}_p$ when $\eta = \left(\frac{-1}{p}\right) = 1$, and $\mathbb{K} = \mathbb{F}_{p^2}$ otherwise. If we put $g(x) = x^4 - (r - 2q)x^2 + q^2$ and let $\mathbb{L}$ be the splitting field of $g(x) \in \mathbb{F}_p[x]$, we have μ_1, $\nu_1 \in \mathbb{L}$ such that $\mu_1 + \nu_1 = \sqrt{r}$ and $\mu_1\nu_1 = q$. Now if $\left(\frac{r}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = 1$, then $\mathbb{L} = \mathbb{F}_p$. Otherwise $\mathbb{L} = \mathbb{F}_{p^2}$. Note that $\mathbb{L}^* = \langle\lambda\rangle$ and if $i = \lambda^{\frac{p-1}{4}}$ when $p \equiv 1 \pmod 4$ or $i = \lambda^{\frac{p^2-1}{4}}$ when $p \equiv -1 \pmod 4$, then $i^2 + 1 = 0$ in $\mathbb{L}$. Thus $i \in \mathbb{L}$ and $\mathbb{L} = \mathbb{K}$.

Theorem 5.1. If $p \nmid 2\Delta Q$, then p has a single rank of apparition in $\{U_n\}$ where U_n is given by (5.1).

Proof. We may write

$$\alpha_1 = i\mu_1^{s+1}, \quad \beta_1 = -i\nu_1^{s+1}, \quad \alpha_2 = iq\mu_1^{s-1}, \quad \beta_2 = -iq\nu_1^{s-1},$$

where μ_1, ν_1, $i \in \mathbb{K}$ and $i^2 + 1 = 0$. Now suppose that ω_1 and ω_2 are defined to be the least positive integers such that in $\mathbb{K}$

$$\alpha_1^{\omega_1} = \alpha_2^{\omega_1} \quad \text{and} \quad (\alpha_1\alpha_2)^{\omega_2} = Q^{\omega_2}$$

respectively. We know that if p has two ranks of apparition in $\{U_n\}$, then either $\omega_1 \nmid \omega_2$ or $\omega_2 \nmid \omega_1$. Now

$$\alpha_1^{\omega_1} = \alpha_2^{\omega_1} \iff (i\mu_1^{s+1})^{\omega_1} = (qi\mu_1^{s-1})^{\omega_1} \iff \mu_1^{2\omega_1} = q^{\omega_1}$$

Also,

$$(\alpha_1\alpha_2)^{\omega_2} = Q^{\omega_2} \iff (i^2q\mu_1^{s-1}\mu_1^{s+1})^{\omega_2} = q^{(s+1)\omega_2} \iff \mu_1^{2s\omega_2} = (-1)^{\omega_2}q^{s\omega_2}$$

We next suppose that $\omega_2 > \omega_1$ and let $\omega_2 = t\omega_1 + u$ with $u \neq 0$ and $-\omega_1/2 \leq u \leq \omega_1/2$. We have

$$\begin{aligned}
\mu_1^{2s(t\omega_1+u)} = (-1)^{t\omega_1+u}q^{s(t\omega_1+u)} \quad &\implies \quad \mu_1^{4s(t\omega_1+u)} = q^{2s(t\omega_1+u)} \\
&\implies \quad \mu_1^{4su}\mu_1^{4st\omega_1} = q^{2st\omega_1}q^{2su} \\
&\implies \quad \mu_1^{2s(2u)} = (-1)^{2u}q^{s(2u)} \\
&\implies \quad (\alpha_1\alpha_2)^{2u} = Q^{2u} \\
&\implies \quad (\alpha_1\alpha_2)^{2|u|} = Q^{2|u|}
\end{aligned}$$

Now $-\omega_1 \leq 2u \leq \omega_1$ implies $|2u| \leq \omega_1 < \omega_2$ which contradicts the definition of ω_2. Suppose now that $\omega_2 < \omega_1$ and let $\omega_1 = t\omega_2 + u$ with $u \neq 0$ and $-\omega_2/2 \leq u \leq \omega_2/2$. Here we have

$$\begin{aligned}
\mu_1^{2(t\omega_2+u)} = q^{t\omega_2+u} \quad &\implies \quad (-1)^{t\omega_2}\mu_1^{2su} = q^{su} \\
&\implies \quad \mu_1^{2s(2u)} = (q^{s(2u)} \\
&\implies \quad (\alpha_1\alpha_2)^{2u} = Q^{2u} \\
&\implies \quad (\alpha_1\alpha_2)^{2|u|} = Q^{2|u|}
\end{aligned}$$

It follows that $|2u| \geq \omega_2$, but since $2|u| \leq \omega_2$, we must have $\omega_2 = 2|u|$ so that $2 \mid \omega_2$. However, in this case we get $\mu_1^{2su} = q^{su}$ and $(\alpha_1\alpha_2)^u = Q^u$ implies that $|u| \geq \omega_2 = 2|u|$, a contradiction. $\square$

We next consider the case of $p \mid 2Q\Delta$. If $p \mid Q$, p can only have one rank of apparition in $\{U_n\}$. If $p \nmid Q$, then if p is odd, $p \mid \Delta$ implies $p \mid t$ or $p \mid v_s^2$. If $p \nmid v_s^2$, then $p \mid t$. [Recall that $\Delta = (4q - r)v_s^2 = t^2 v_s^2$.] If $p \mid E$, then $p \mid v_{s-1}v_{s+1}$ and since

$$v_s^2 - v_{s-1}v_{s+1} = t^2 q^{s-1}$$

we get $p \mid v_s^2$, a contradiction. Thus, if $p \mid \Delta$ and $p \mid E$, then $p \mid v_s^2$ and $p \mid v_{s-1}v_{s+1}$; therefore $p \mid t^2 q^{s-1}$ which implies $p \mid t$. Now since

$$v_s^2 + t^2 u_s^2 = 4q^s$$

we get $p \mid 4q$ so that $p = 2$, a contradiction. We have shown that if p is odd and $p \mid \Delta$, then $p \nmid E$, which implies that p has two ranks of apparition in $\{U_n\}$. Thus, $\{U_n\}$, where U_n is given by (5.1), can be monoapparitic only when $|\Delta| = 2^{2k}$.

We have seen that if U_n is given by (5.1), then all primes, except possibly 2, can have only one rank of apparition in $\{U_n\}$ when $|\Delta| = 2^{2k}$. We next show that if $|\Delta| = 2^{2k}$, then 2 can have only one rank of apparition in $\{U_n\}$. Since $|\Delta| = 2^{2k}$, we have $|tv_s| = 2^k$. If $2 \mid t$, then $2 \mid P_1$ and $2 \mid P_2$. If $2 \nmid t$, then $|t| = 1$ and if $2 \mid s$, we get $2 \nmid U_s$ so that $2 \nmid P_1$. If $2 \nmid s$, then r is a perfect square, say $r = m^2$, and $2 \nmid m$. Now $v_1 = \pm m$ and $v_1 \mid v_s$ implies $m \mid v_s$ which implies $|m| = 1$ (m is odd). Thus, $r = m^2 = 1$ and since $4q - r = t^2$, we have a contradiction.

Consider the special case of $s = 2$. Here we have

$$\Delta = t^2(2q - t^2)^2, \quad E = q^2(t^2 - 4q)^2(t^2 - q)^2, \quad P_1 = t(t^2 - 4q),$$

$$P_2 = -t^2 q(t^2 - 3q), \quad Q = q^3$$

For this $\{U_n\}$ sequence to be monoapparitic, we require

$$t(2q - t^2) = \pm 2^k$$

Hence $t = \epsilon\, 2^u$, $2q - t^2 = \eta\, 2^v$, where $|\epsilon| = |\eta| = 1$. If $u = 0$, then $2q = 1 + \eta\, 2^v$ implies $v = 0$ and $q = \frac{1+\eta}{2}$. If $\eta = -1$, then $q = 0$ implies that $E = 0$, contradicting $D \neq 0$. If $\eta = 1$, then $q = 1$ and $t^2 = 1$ implies that $E = 0$, a contradiction. Then $u > 0$ implies $q = 2^{2u-1} + \eta 2^{u-1}$, $t = \epsilon 2^u$. In the case of $s = u = \epsilon = \eta = 1$, we get $t = 2$, $q = 3$ and $P_1 = 16$, $P_2 = 60$, $Q = 27$. We know that the associated sequence is monoapparitic.

6. The Case When E Is Not a Square

We initiated a computer search to discover likely monoapparitic sequences $\{U_n\}$. Several were discovered and we found that most of these satisfied the condition that $\alpha_2/\beta_2 = \zeta_k$, where ζ_k is a k-th root of unity with $k = 3$ or 4. For each of the discovered sequences, E is not a perfect square. For such sequences we have

$$\begin{aligned} \rho_2 &= \alpha_2 + \beta_2 = \beta_2(1+\zeta_k) \\ P_1 &= \beta_2(1+\zeta_k) + \rho_1 \\ P_2 &= \rho_1\beta_2(1+\zeta_k) \end{aligned}$$

Hence

$$\rho_2 = \beta_2(1+\zeta_k) = \frac{P_1 + \epsilon\sqrt{\Delta}}{2}, \quad \text{where } \epsilon = \pm 1, \text{ and}$$

$$\frac{1}{\beta_2} = \frac{(1+\zeta_k)(P_1 - \epsilon\sqrt{\Delta})}{2P_2}$$

Since $\alpha_2 = Q/\beta_2$ we get

$$\zeta_k = \frac{\alpha_2}{\beta_2} = \frac{Q(1+\zeta_k)^2(P_1 - \epsilon\sqrt{\Delta})}{P_2(P_1 + \epsilon\sqrt{\Delta})} = \frac{4(1+\zeta_k)^2 Q}{(P_1 + \epsilon\sqrt{\Delta})^2}$$

It follows that

$$\left(\frac{P_1 + \epsilon\sqrt{\Delta}}{2}\right)^2 \Big/ Q = \frac{(1+\zeta_k)^2}{\zeta_k} = 2 + \frac{1}{\zeta_k} + \zeta_k \tag{6.1}$$

Suppose that $\alpha_2/\beta_2 = \zeta_k$ for any k. We must have $\frac{1}{\zeta_k} + \zeta_k \in \mathbb{Q}(\sqrt{\Delta})$. Since $\zeta_k + \frac{1}{\zeta_k}$ must be a zero of an irreducible polynomial in $\mathbb{Z}[x]$ of degree $\phi(k)/2$, we must have $\phi(k)/2 \leq 2$ or $k \in \{1,2,3,4,5,6,8,10,12\}$. Since $\alpha_2 \neq \beta_2$ ($D \neq 0$), we cannot have $k = 1$. Also, if Δ is not an integer square, then $k \in \{5,8,10,12\}$. It is an easy matter to eliminate the values 10 and 8 for k because $P_1^2/P_2 \notin \mathbb{Q}$ in these cases. When $k = 12$ we find that from (6.1) we get $(P_1, P_2, Q) \neq 1$, and when $k = 5$, we find that either $P_1^2 = -P_2$, $Q = P_2$ or $P_1^2 = 5P_2$, $Q = P_2$. In the second case we get $5 \mid (P_1, P_2, Q)$ and in the first case we can take $P_1 = 1$, $P_2 = -1$, $Q = 1$ or $P_1 = -1$, $P_2 = -1$, $Q = 1$. However, neither of these cases is very interesting because the resulting $\{U_n\}$ sequences are purely periodic with period 10 with $U_{10k} = 0$ and $|U_k| = 1$ ($10 \nmid k$). This sequence is, however, trivially monoapparitic. Thus, the possibilities for k narrow down to the set $\{2,3,4,6\}$.

We now consider the posibility that $k = 6$. We have $\zeta_6 + \zeta_6^{-1} = 1$ and

$$\left(\frac{P_1 + \epsilon\sqrt{\Delta}}{2}\right)^2 = 3Q$$

It follows that $\sqrt{\Delta} \in \mathbb{Z}$ and we put $\Delta = S^2$ for some $S \in \mathbb{Z}$. We then get $Q = 3R^2$ with $R \in \mathbb{Z}$ and $P_1 + S = 6R$. Since $P_1^2 - 4P_2 = S^2$ we find that $P_2 = 9R^2 - 3RS$. Hence,

$$U_2 = P_1 = 6R - S, \qquad U_3 = P_1^2 - P_2 - 3Q = (6R - S)(3R - S)$$

Thus, if p is a prime and $p \mid (6R - S)$, then $p \mid U_2$ and $p \mid U_3$ and $\{U_n\}$ cannot be monoapparitic. Thus, $P_1 = 6R - S = \pm 1$. In this case we have $S = 6R \mp 1$, $\Delta = (6R \mp 1)^2$, $P_2 + 4Q = 3R^2 \pm 3R$ and $E = 3R^2(3R^2 \pm 6R - 1)$. If p is a prime and $p \mid \Delta$, then if $p \mid E$, we get $p \mid 3R$ which implies $p \nmid \Delta$, a contradiction. Thus, if $p \mid \Delta$, p must have two ranks of apparition in $\{U_n\}$. It follows that $\Delta = (6R \pm 1)^2 = 1$, which implies $R = 0$, and hence $E = 0$, which is impossible. Thus, if $\alpha_2/\beta_2 = \zeta_k$ and $\{U_n\}$ is monoapparitic, it is necessary that $k \in \{2, 3, 4\}$. These cases are covered in the following theorem.

Theorem 6.1. Suppose $\alpha_2/\beta_2 = \zeta_k$, where $k \in \{2, 3, 4\}$. Let p be any prime such that $p \nmid 2\Delta Q$ and let ω be the least positive integer such that $p \mid U_\omega$. If $p \mid U_m$ for any positive integer m, then $\omega \mid m$.

Proof. As usual, let $\mathbb{K}$ denote the splitting field of $F(x) \in \mathbb{F}_p[x]$. In $\mathbb{K}$ we have $\alpha_1 + \beta_1 \neq \alpha_2 + \beta_2$ $(p \nmid \Delta)$ and

$$\alpha_1^\omega + \beta_1^\omega = \alpha_2^\omega + \beta_2^\omega \quad \text{and} \quad \alpha_1^\omega \beta_1^\omega = \alpha_2^\omega \beta_2^\omega$$

By renaming α_1 and β_1, we may assume with no loss of generality that $\alpha_1^\omega = \alpha_2^\omega$ and $\beta_1^\omega = \beta_2^\omega$. Now let $m = q\omega + r$, where $0 \leq r < \omega$. If $r = 0$, then $\omega \mid m$ and we are done. Suppose that $r \neq 0$. Since

$$\alpha_1^m + \beta_1^m = \alpha_2^m + \beta_2^m \quad \text{and} \quad \alpha_1^m \beta_1^m = \alpha_2^m \beta_2^m$$

we have either $\alpha_1^m = \alpha_2^m$ or $\alpha_1^m = \beta_2^m$. If $\alpha_1^m = \alpha_2^m$, then

$$\alpha_1^r \alpha_1^{q\omega} = \alpha_2^r \alpha_2^{q\omega} \implies \alpha_1^r = \alpha_2^r \implies \beta_1^r = \beta_2^r \implies U_r = 0 \in \mathbb{K}$$

Since $p \mid U_r$ and $r < \omega$, we have a contradiction. Thus we must have

$$\begin{aligned}
\alpha_1^m = \beta_2^m \quad &\implies \quad \alpha_1^{q\omega+r} = \beta_2^{q\omega+r} \\
&\implies \quad \alpha_1^{q\omega}\alpha_1^r = \beta_2^r \beta_2^{q\omega} \\
&\implies \quad \alpha_1^r = (\beta_2/\alpha_1)^{q\omega}\beta_2^r = (\beta_2/\alpha_2)^{q\omega}\beta_2^r \\
&\implies \quad \alpha_1^r = \zeta_k^{-q\omega}\beta_2^r \\
&\implies \quad \beta_1^r = \zeta_k^{q\omega}\alpha_2^r \\
&\implies \quad \beta_1^{kr} = \alpha_2^{kr} \\
&\implies \quad \alpha_1^{kr} = \beta_2^{kr} \\
&\implies \quad U_{kr} = 0 \in \mathbb{K}
\end{aligned}$$

Thus, since $p \mid U_{kr}$, we must have $\omega \leq kr$.

If $k \mid \omega$, then $\zeta_k^\omega = 1$ and we can prove that $U_r = 0 \in \mathbb{K}$, which is a contradiction. Hence we may assume that $0 < \omega < kr$ and $k \nmid \omega$.

Let $kr = t\omega + s$, where $0 \le s < \omega$. Since $t\omega \equiv -s \pmod{k}$, we get $\zeta_k^{t\omega} = \zeta_k^{-s}$. If $s > 0$, then

$$\begin{aligned} \beta_1^{t\omega+s} = \alpha_2^{t\omega+s} \quad &\Longrightarrow \quad \beta_1^s = \alpha_2^s(\alpha_2/\beta_2)^{t\omega} \\ &\Longrightarrow \quad \beta_1^s = \alpha_2^s\zeta_k^{t\omega} \;=\; \alpha_2^s\zeta_k^{-s} \;=\; \beta_2^s \end{aligned}$$

Hence $\alpha_1^s = \alpha_2^s$ and $p \mid U_s$. As this contradicts the definition of ω, we can only have $s = 0$ and $kr = t\omega$. Since $\omega > r$, we have $0 < t < k$. If $k = 2$ or 3, then, since $(t, k) = 1$, we have $k \mid \omega$, which is not possible. If $k = 4$, then $k \nmid \omega$, so that $\omega = 2r$ and $2 \nmid r$. In this case we get $m = r(2q + 1)$ and

$$\alpha_1^{2r} = \alpha_2^{2r} \implies \alpha_1^r = -\alpha_2^r \implies \alpha_1^m = -\alpha_2^m$$

However, we know that $\alpha_1^m = \beta_2^m$ and this means that

$$-\alpha_2^m = \beta_2^m \implies (\alpha_2/\beta_2)^m = -1 \implies \zeta_4 = -1$$

Since $2 \nmid m$, this is impossible. It follows that we can only have $r = 0$ and $\omega \mid n$. $\square$

If we consider the case of $k = 2$, we have $\zeta_k = -1$ and we must have

$$\left(\frac{P_1 + \epsilon\sqrt{\Delta}}{2}\right)^2 \bigg/ Q = 0$$

Hence $\Delta = P_1^2$ and $P_2 = 0$. We get $\rho_2 = 0, \rho_1 = P_1$, and

$$\alpha_2 = \sqrt{-Q},\ \beta_2 = -\sqrt{-Q},\ \alpha_2^n + \beta_2^n = \begin{cases} 0 & \text{when } 2 \nmid n \\ 2(-1)^{n/2}Q^{n/2} & \text{when } 2 \mid n \end{cases}$$

In this case we find that

$$\left.\begin{aligned} U_{2n+1} &= v_{2n+1}(P_1, Q)/P_1 \\ U_{4n+2} &= v_{2n+1}^2(P_1, Q)/P_1 \\ U_{4n} &= (P_1^2 - 4Q)u_{2n}^2(P_1, Q)/P_1 \end{aligned}\right\} \qquad (6.2)$$

and $E = 16Q^2 - 4QP_1^2$ need not be a perfect square. Now if $p \mid \Delta$, we must have $p \mid E$ in order that $\{U_n\}$ should be monoapparitic. It follows that $|\Delta| = 2^{2h}$ with $h \ge 0$. Thus, if $\{U_n\}$ is given by (6.2), it will be monoapparitic when

$$P_1 = \pm 1, \quad P_2 = 0, \quad Q \in \mathbb{Z} \qquad \text{or} \qquad P_1 = \pm 2^h, \quad P_2 = 0, \quad Q \in \mathbb{Z},\ 2 \nmid Q$$

If $k = 3$, then

$$\left(\frac{P_1 + \epsilon\sqrt{\Delta}}{2}\right)^2 \bigg/ Q = 1;$$

hence, $\Delta = S^2$ and $Q = R^2$ with $S, R \in \mathbb{Z}$. We get $P_1 = 2R - S$, $P_2 = R^2 - RS$. Since $(P_1, P_2, Q) = 1$ we must have $(R, S) = 1$. Also, $E = 3R^2(3R - S)(R + S)$

need not be a perfect square. Furthermore, we must have $|S| = 3^h$ with $h \geq 0$ and $3 \nmid R$ when $3 \mid S$. In this case, it is a simple matter to show that E can only be a perfect square when $h > 1$ and $R = \pm 3^{2h-2} + 1 - S/3$.

If $k = 4$, then

$$\left(\frac{P_1 + \epsilon\sqrt{\Delta}}{2}\right)^2 \Big/ Q = 2;$$

and $Q = 2R^2$, $\Delta = S^2$, where $R, S \in \mathbb{Z}$. We get $P_1 = 4R - S$, $P_2 = 4R^2 - 2RS$ and $(2R, S) = 1$. Also $E = 2R^2(4R^2 + 4RS - S^2)$ is not a perfect square. Here, in order to ensure that $\{U_n\}$ is monoapparitic we must have $|S| = 1$.

Thus, we have established that there exists an infinitude of monoapparitic sequences $\{U_n\}$ for which Δ is a square and E is not.

7. The Case When Neither Δ Nor E Is a Perfect Square

There remains the case in which neither Δ nor E is a perfect square. However, in this case we must have ΔE a perfect square, which means that $\Delta = GU^2$, $E = GV^2$ with $G, U, V \in \mathbb{Z}$; G is squarefree and $G \neq 1$.

Theorem 7.1. If G is defined as above, then G must be the sum of two integer squares.

Proof. Let $H = (U, V)$. Put $S = U/H$, $T = V/H$. From the definition of E and Δ it is a simple matter to produce the identity $(P_2 - 4Q)^2 - 4Q\Delta = E$. Hence

$$(P_2 - 4Q)^2 - 4QGH^2S^2 = GH^2T^2$$

It follows that $GH \mid P_2 - 4Q$. On putting $W = (P_2 - 4Q)/GH$ we get

$$GW^2 - 4QS^2 = T^2$$

Thus, $Q = (GW^2 - T^2)/4S^2$, $P_2 = GHW + (GW^2 - T^2)/S^2$ and

$$P_1^2 = \Delta + 4P_2 = GH^2S^2 + 4(GHW + (GW^2 - T^2)/S^2)$$

Hence

$$S^2P_1^2 - 4GHWS^2 - 4GW^2 + 4T^2 - GH^2S^4 = 0$$

or

$$\begin{aligned} S^2P_1^2 + 4T^2 &= G(4W^2 + 4HWS^2 + H^2S^4) \\ &= G(HS^2 + 2W)^2 \end{aligned}$$

If we put $Y = SP_1$, $X = HS^2 + 2W$, we get $Y^2 + 4T^2 = GX^2$. If $D = (Y, 2T)$, then $D^2 \mid GX^2$, which implies $D \mid X$. Now if $Y' = Y/D$, $Z' = 2T/D$, $X' = X/D$, we get $Y'^2 + Z'^2 = GX'^2$, where $(Y', Z') = 1$. Thus, if p is any prime divisor of G, we have that $p = 2$ or $\left(\frac{-1}{p}\right) = 1$ which implies $p \equiv 1 \pmod 4$. Since $G > 0$, we see that G must be the sum of two squares. □

Theorem 7.2. Under the conditions of the theorem we must have

$$P_1 = Y/S, \qquad P_2 = \left((Y/S)^2 - GH^2S^2\right)/4$$
$$Q = \left((Y/S)^2 - 2GHX + GH^2S^2\right)/16$$

Here $S = U/H$, where $H = (U, V)$. Also, $Y^2 + 4T^2 = GX^2$, $S \mid Y$, $T = V/H$, $Y/S \equiv HS \pmod 2$ and $X \equiv HS^2 + 2T \pmod 4$.

Proof. We have already seen in the proof of the theorem that $S \mid Y$ and $P_1 = Y/S$. Also, since $4P_2 = P_1^2 - \Delta$, we get

$$4P_2 = (Y/S)^2 - GH^2S^2 \quad \text{and} \quad (Y/S)^2 \equiv GH^2S^2 \pmod 4$$

If $2 \mid HS$, then $2 \mid Y/S$ and $Y/S \equiv HS \pmod 2$. If $2 \nmid HS$, then $(Y/S)^2 \equiv G \pmod 4$. Since G is squarefree, we must have $G \equiv 1 \pmod 4$ and

$$(Y/S)^2 \equiv H^2S^2 \pmod 4$$

It follows that $Y/S \equiv HS \pmod 2$. Finally, we know that

$$4Q = (GW^2 - T^2)/S^2$$

where $W = (X - HS^2)/2$. Substituting for W in the above expression, we get

$$\begin{aligned} 4Q &= (GX^2 - 4T^2 - 2GHXS^2 + GH^2S^4)/4S^2 \\ &= (Y^2 - 2GHS^2X + GH^2S^4)/4S^2 \end{aligned}$$

Thus, $Q = ((Y/S)^2 - 2GHX + GH^2S^2)/16$. Also, since $4 \mid GW^2 - T^2$, we find that $T \equiv W \pmod 2$ when G is odd, and $2 \mid T$ when G is even. Since G is squarefree, we get $2 \mid W$ when $2 \mid T$; thus, $T \equiv W \pmod 2$ and $X = HS^2 + 2W \equiv HS^2 + 2T \pmod 4$. □

With some additional work it is possible to prove the following result, which, for brevity, we only state here.

Theorem 7.3. If $\Delta = GH^2S^2$, $E = GH^2T^2$, where G is squarefree and $(S, T) = 1$, it is necessary and sufficient that P_1, P_2 and Q be given by

$$P_1 = Y/S, \quad P_2 = ((Y/S)^2 - GH^2S^2)/4, \quad Q = ((Y/S)^2 - 2GHX + GH^2S^2)/16$$

where $X, Y, G, H, S, T \in \mathbb{Z}$; $Y^2 + 4T^2 = GX^2$; $S \mid Y$; $G \equiv 1 \pmod 4$ unless $2 \nmid S$ and $4 \mid H$; $Y/S \equiv HS \pmod 2$; $X \equiv HS^2 + 2T \pmod 4$; and one of the following conditions holds.

i) $2 \nmid HS$
ii) $2 \nmid S$, $4 \mid H$, $4 \mid Y/S$
iii) $2 \nmid S$, $2 \| H$, $2 \| Y/S$, $H \equiv X \pmod 4$
iv) $2 \nmid S$, $2 \| H$, $4 \mid Y/S$, $X \equiv H/2 \pmod 4$
v) $2 \| S$, $4 \mid Y/S$, $4 \mid H$
vi) $2 \| S$, $4 \mid Y/S$, $H \equiv X/2 \pmod 4$
vii) $4 \mid S$, $4 \mid Y/S$, $4 \mid H$
viii) $4 \mid S$, $4 \nmid Y/S$, $H \equiv X/2 \pmod 4$

Consider the example $H = S = Y = 1$. In this case we have $\Delta = G$, $E = GT^2$, $G \equiv 1 \pmod 4$, $X \equiv 3 \pmod 4$, and

$$P_1 = Y, \quad P_2 = (Y^2 - G)/4, \quad Q = (Y^2 - 2GX + G)/16$$

where $4T^2 - GX^2 = -1$. If we put $G = 5$, $T = 1$, $X = -1$, we get $P_1 = 1$, $P_2 = -1$, $Q = 1$, a case considered in **§6**.

If we put $T = 19$, $X = -17$, then $P_1 = 1$, $P_2 = -1$, $Q = 11$. However, for these values of P_1, P_2 and Q we find that the prime 61 has two ranks of apparition, 12 and 30, in $\{U_n\}$. Thus, $\{U_n\}$ is not monoapparitic.

8. Open Questions

1) Have we found all examples of monoapparitic sequences $\{U_n\}$ for which E is a perfect square?
2) Have we found all examples of monoapparitic $\{U_n\}$ for which E is not a perfect square and Δ is.
3) Do there exist any nontrivial monoapparitic $\{U_n\}$ such that neither Δ nor E is a perfect square?

Acknowledgement. We would like to thank a very discerning referee for enabling us to remove several obscurities and minor errors.

References

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

[2] Paulo Ribenboim, *The New Book of Prime Number Records*, Springer, New York, 3rd edition, 1995.

[3] 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,

[4] Hugh C. Williams & Richard K. Guy, Some fourth order linear divisibility sequences, *Internat. J. Number Theory*, **7**, No. 5 (2011) 1255–1277.