FIXED POINTS AND UPPER BOUNDS FOR THE RANK OF APPEARANCE IN LUCAS SEQUENCES

LAWRENCE SOMER AND MICHAL KŘÍŽEK

Abstract. Let $U(P,Q)$ denote the Lucas sequence satisfying the recursion relation

$$U_{n+2} = PU_{n+1} - QU_n,$$

where $U_0 = 0$, $U_1 = 1$, and P and Q are integers. Let $z(n)$, called the rank of appearance of n in $U(P,Q)$, denote the least positive integer m such that $U_m \equiv 0 \pmod{n}$. We find all fixed points n for the rank of appearance such that $z(n) = n$. We also show that $z(n) \le 2n$ when $z(n)$ exists. This paper improves results considered by Diego Marques regarding the Fibonacci sequence.

1. Introduction

Consider the Lucas sequence $(U) = U(P,Q)$ which satisfies the second order recursion relation

$$U_{n+2} = PU_{n+1} - QU_n \tag{1.1}$$

with initial terms $U_0 = 0$, $U_1 = 1$, where P and Q are integers and $D = P^2 - 4Q$ is the discriminant of $U(P,Q)$. We let $V(P,Q)$ denote the companion Lucas sequence which satisfies the same recursion relation (1.1) as $U(P,Q)$ and has initial terms $V_0 = 2$ and $V_1 = P$. Associated with $U(P,Q)$ and $V(P,Q)$ is the characteristic polynomial

$$f(x) = x^2 - Px + Q \tag{1.2}$$

with characteristic roots α and β. By the Binet formulas,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ if } D \ne 0. \tag{1.3}$$

Moreover,

$$U_n = n\alpha^{n-1} \text{ if } D = 0, \tag{1.4}$$

where α is an integer if $D = 0$, and

$$V_n = \alpha^n + \beta^n. \tag{1.5}$$

It is known (see [3, pp. 344–345]), that if $\gcd(n,Q) = 1$, then $U(P,Q)$ is purely periodic modulo n. Since $U_0 = 0$, it follows that there exists a least positive integer m such that $U_m \equiv 0 \pmod{n}$ when $\gcd(n,Q) = 1$. This integer m, which is denoted by $z(n)$, is called the *rank of appearance* of n in $U(P,Q)$.

Marques [6] discussed when $z(n) = n$ for the Fibonacci sequence $U(1,-1)$. He also gave an upper bound of $(n-1)^2$ for $z(n)$. In this paper, we generalize some of these results from the Fibonacci sequence to the general Lucas sequence $U(P,Q)$. In particular, we determine all instances in which $n \mid z(n)$. We show this can happen only when $z(n) = n$, and n is a fixed point of the function z, or when $z(n) = 2n$. We accomplish this by showing that $2n$ is an upper bound for $z(n)$ when $z(n)$ exists, improving the bound given in [6] for the Fibonacci sequence. We further exhibit infinitely many Lucas sequences $U(P,Q)$ for which $U_n \neq 0$ for $n \geq 1$ and $z(n) \leq n$ for all $n \geq 1$ when $z(n)$ is defined. In particular, we find infinitely many Lucas sequences $U(P,Q)$ for which $U_n \neq 0$ for $n \geq 1$ and $z(n) < n/2$ for all $n > 4$. In addition, we show that if $D = 1$, then there are no integers $n > 1$ such that either $z(n) \mid n$ or $n \mid z(n)$. Moreover, when $Q = 0$ or $U_n = 0$ for some $n \geq 1$, we demonstrate that either $z(n) \leq 1 + \lceil \log_2 n \rceil$ when $z(n)$ exists or $z(n) \leq 6$ for all $n \geq 1$.

We note that there are some incorrect statements in [6] in some of the proofs and results. We provide some corrections for this paper at the end of our article. A key tool in the determination of positive integers n for which $z(n) = n$ will be Theorem 1.1 due to Chris Smyth [8] in which he gives necessary and sufficient conditions for ascertaining when $n \mid U_n$. Before presenting this theorem, we need a few definitions. We let S be the set of all n such that $n \mid U_n(P,Q)$. For $n \in S$, define $\mathcal{P}_{S,n}$ to be the set of primes p such that $np \in S$. An element $n \in S$ is said to be *basic* if there is no prime p such n/p is in S.

Theorem 1.1.

(a) For $n \in S$, the set $\mathcal{P}_{S,n}$ is the set of primes dividing DU_n.

(b) Every element of S can be written in the form $bp_1 \cdots p_r$ for some $r \geq 0$, where $b \in S$ is basic and, for $i = 1, \ldots, r$, the positive integers $bp_1 \cdots p_{i-1}$ are also in S, and p_i is in $\mathcal{P}_{S,bp_1\cdots p_{i-1}}$.

(c) The basic elements of S are:

(i) 1 *and* 6 *if* $P \equiv 3 \pmod 6$, $Q \equiv \pm 1 \pmod 6$,
(ii) 1 *and* 12 *if* $P \equiv \pm 1 \pmod 6$, $Q \equiv -1 \pmod 6$,
(iii) 1 *only, otherwise.*

We note that the primes p_i in part (b) of Theorem 1.1 need not be distinct.

Throughout this paper, p will denote a prime. We say that p is a *special prime* with respect to the Lucas sequence $U(P,Q)$ if $p \mid P$ and $p \mid Q$. Note that $p \mid D$ if p is a special prime.

We also define p to be an *irregular prime* with respect to $U(P,Q)$ if $p \mid Q$ but $p \nmid P$; otherwise, p is called *regular*. We note that if $p \mid D$, then p is a regular prime. We shall see later in Proposition 3.1 (xiii) that $z(n)$ does not exist if and only if n has an irregular prime divisor. The prime p is a *primitive prime divisor* of U_n if $p \mid U_n$ but $p \nmid U_m$ for $0 < m < n$.

The Lucas sequence $U(P,Q)$ is called *degenerate* if $PQ = 0$ or if α/β is a root of unity. Since α and β are the zeros of a quadratic polynomial with integer coefficients, it follows that α/β can be an nth root of unity only if $n \in \{1,2,3,4,6\}$. It follows from (1.3) and (1.4) that U_n can equal 0 for $n \geq 1$ only if (U) is a degenerate sequence.

For later reference, we characterize all degenerate Lucas sequences in Theorem 1.2.

Theorem 1.2. *Suppose that $U(P,Q)$ is a degenerate Lucas sequence with discriminant D and characteristic roots α and β.*

(i) *If $P = Q = 0$, then $U_n = 0$ for $n \geq 2$, and $D = 0$.*
(ii) *If $P \neq 0$ and $Q = 0$, then $U_n = P^{n-1}$ for $n \geq 1$, and $D = P^2$.*
(iii) *Suppose that $\alpha/\beta = 1$. Then $D = 0$ and $P = 2N$, $Q = N^2$ for some nonzero integer N. Moreover, $U_n = nN^{n-1}$ for $n \geq 0$.*
(iv) *Suppose that $\alpha/\beta = -1$. Then $P = 0$ and $Q = N$ for some nonzero integer N. Moreover, $D = -4N$, $U_{2n} = 0$, and $U_{2n+1} = (-Q)^n$ for $n \geq 0$.*
(v) *Suppose that α/β is a primitive cube root of unity. Then $P = N$ and $Q = N^2$ for some nonzero integer N. Further, $U_{3n} = 0$, $U_{3n+1} = (-1)^n P^{3n}$, $U_{3n+2} = (-1)^n P^{3n+1}$ for $n \geq 0$, and $D = -3N^2$.*

(vi) *Suppose α/β is a primitive fourth root of unity. Then $P = 2N$ and $Q = 2N^2$ for some nonzero integer N. Further, $D = -4N^2$ and $U_{4n} = 0$, $U_{4n+1} = (-1)^n(2N^2)^{2n}$, $U_{4n+2} = (-1)^n 2^{2n+1}N^{4n+1}$, $U_{4n+3} = (-1)^n 2^{2n+1}N^{4n+2}$ for $n \geq 0$.*

(vii) *Suppose α/β is a primitive sixth root of unity. Then $P = 3N$ and $Q = 3N^2$ for some nonzero integer N. Furthermore, $D = -3N^2$ and $U_{6n} = 0$, $U_{6n+1} = (-1)^n(3^3N^6)^n$, $U_{6n+2} = (-1)^n 3^{3n+1}N^{6n+1}$, $U_{6n+3} = (-1)^n 2{\cdot}3^{3n+1}N^{6n+2}$, $U_{6n+4} = (-1)^n 3^{3n+2}N^{6n+3}$, $U_{6n+5} = (-1)^n 3^{3n+2}N^{6n+4}$ for $n \geq 0$.*

Proof. Parts (i) and (ii) follow by inspection. For parts (iii)–(vii), the forms for P and Q are given by Ward [10, p. 613]. The terms U_n are given by Theorem 9 of [9]. □

2. Main Results

Now we will survey our main results. The proofs not given in this section will be presented in Section 4.

Theorem 2.1. *Consider the Lucas sequence $U(P,Q)$. Let b be a basic element of $U(P,Q)$ and let $d = \gcd(P,Q)$. Let $R \geq 1$ denote an integer such that each prime divisor of R also divides D. Then $z(n) = n$ if and only if exactly one of the following holds:*

(i) $\gcd(n,d) = 1$ *and* $n = bR$, *where* $4 \nmid R$ *if* $4 \mid P$ *and* $9 \nmid R$ *if* $P^2 \equiv Q \pmod 9$,

(ii) $2 \mid \gcd(n,d)$ *and* $n = 2$,

(iii) $P \equiv Q \equiv 2 \pmod 4$ *and* $n = 4$.

The following corollary is stated as Theorem 1.1 in [6] and was conjectured by Benoit Cloitre according to [6, p. 346].

Corollary 2.2. *Consider the Fibonacci sequence $\{F_n\} = U(1,-1)$. Then $z(n) = n$ if and only if $n = 5^k$ or $12 \cdot 5^k$ for some $k \geq 0$.*

Corollary 2.2 immediately follows from Theorems 1.1 and 2.1 upon noting that $P \equiv 1 \pmod 6$, $Q \equiv -1 \pmod 6$, $d = 1$, and $D = 5$.

Theorem 2.3 gives a best upper bound for $z(n)$ when $z(n)$ exists.

Theorem 2.3. *Consider the Lucas sequence $U(P,Q)$ and let $d = \gcd(P,Q)$. Let $R \geq 1$ denote an integer such that each prime divisor of R divides D. Then $z(n)$ does not exist if and only if n has an irregular prime divisor, and $z(n) \leq 2n$, otherwise. Moreover, $z(n) = 2n$ if and only if $P \equiv \pm 1 \pmod 6$, $Q \equiv -1 \pmod 6$, $\gcd(n,d) = 1$, and $n = 6R$. Further, $n \mid z(n)$ only if $z(n) = n$ or $z(n) = 2n$.*

Corollary 2.4. *Consider the Lucas sequence $U(P,Q)$. If $z(n)$ exists and $z(n) < 2n$, then $z(n) \leq \frac{12}{7}n$.*

Theorem 2.5 below sharpens Theorem 2.3 by exhibiting infinitely many Lucas sequences $U(P,Q)$ for which $U_n \neq 0$ for $n \geq 1$, $Q \neq 0$, and $z(n) \leq n$ for $n \geq 1$ when $z(n)$ exists. In part (v) of Theorem 2.5, we find infinitely many such Lucas sequences for which we have the better upper bound of $z(n) < n/2$ for all $n > 4$. We define the *radical* of n for $n \geq 1$, denoted by $\operatorname{rad}(n)$, to be the product of the distinct primes dividing n. By convention, $\operatorname{rad}(1) = 1$.

Theorem 2.5. *Let $U(P,Q)$ be a Lucas sequence and let $d = \gcd(P,Q)$.*

(i) *Suppose that $Q = \frac{P^2-r^2}{4}$ for some $r \geq 1$ and $P \neq 0$ such that $P \equiv r \pmod 2$ and $P \neq \pm r$. Then $U(P,Q)$ is nondegenerate, $D = r^2$, and $z(n) \leq n$ if n has no irregular prime divisors. In particular, if P is odd, then $z(n)$ does not exist if $2 \mid n$. Moreover, if $r = 1$, then $z(n) < n$ if n has no irregular prime divisors.*

(ii) *Suppose that $Q = r^2$ for some $r \geq 1$ and that $P \neq 0$, $\pm r$, or $\pm 2r$. We further suppose that if r is odd, then $2 \mid P$. Then $U(P,Q)$ is nondegenerate, $D = P^2 - 4r^2$, and $z(n) \leq n$ whenever $z(n)$ exists.*

(iii) *Suppose that $P = 2N$ and $Q = N^2$ for some nonzero integer N. Then $D = 0$, $U_n = nN^{n-1}$, and $z(n) \leq n$ for all $n \geq 1$. Moreover, $z(n) = n$ if $\gcd(n,N) = 1$.*

(iv) *Suppose that $P = d_1P_1$ and $Q = d_1^2Q_1^2$, where $Q_1 \geq 1$, $\gcd(P_1,Q_1) = 1$, $d_1 \neq 0$, $12 \mid d_1$, $P_1 \neq 0$, $(P_1,Q_1) \neq (\pm 1, 1)$ or $(\pm 2, 1)$, and $\mathrm{rad}(P_1Q_1(P_1^2 - 4Q_1^2)) \mid d_1$. Then $U(P,Q)$ is nondegenerate, $Q = (d_1Q_1)^2$, $D = d_1^2(P_1^2 - 4Q_1^2)$,*

$$\mathrm{rad}(P) = \mathrm{rad}(Q) = \mathrm{rad}(D), \tag{2.1}$$

and $z(n)$ exists for $n \geq 1$. Moreover, $z(n) \leq \frac{3}{5}n$ for $n \geq 4$. In addition, $z(n) \leq n$ for $n \geq 1$ and $z(n) \leq \frac{2}{3}n$ for $n \geq 3$.

(v) *Suppose that (t, Q_1, P_1) is a primitive Pythagorean triple, where $4 \mid Q_1$. Let $P = d_2P_1$ and $Q = d_2^2\big(\frac{Q_1}{2}\big)^2$, where $d_2 \neq 0$, $4 \mid d_2$, and $\mathrm{rad}(tQ_1P_1) \mid d_2$. Then $U(P,Q)$ is nondegenerate, $60 \mid d_2$, $Q = \big(d_2\frac{Q_1}{2}\big)^2$,*

$$D = P^2 - 4Q = d_2^2(P_1^2 - Q_1^2) = (d_2t)^2, \tag{2.2}$$

and

$$\mathrm{rad}(P) = \mathrm{rad}(Q) = \mathrm{rad}(D). \tag{2.3}$$

Moreover, $z(n) < \frac{n}{2}$ for $n > 4$. In addition, $z(n) \leq \frac{n}{2}$ for $n \geq 4$ and $z(n) \leq n$ for $n \geq 1$.

Example 2.6. We exhibit a Lucas sequence $U(P,Q)$ which satisfies the conditions of part (v) of Theorem 2.5. Consider the primitive Pythagorean triple $(t, Q_1, P_1) = (3, 4, 5)$. Let $d_2 = 60$. Then $4 \mid d_2$ and $\mathrm{rad}(3 \cdot 4 \cdot 5) = 30 \mid d_2$. Let $P = d_2P_1 = 300$ and $Q = d_2^2\big(\frac{Q_1}{2}\big)^2 = 14400$. Then

$$D = P^2 - 4Q = 300^2 - 4 \cdot 14400 = 32400 = 180^2 = (d_2t)^2.$$

By Theorem 2.5, we see that for the Lucas sequence $U(300, 14400)$, we have $z(n) \leq \frac{n}{2}$ for $n \geq 4$ and $z(n) < \frac{n}{2}$ for $n \geq 5$.

Corollary 2.7. *Consider the Lucas sequence $U(P,Q)$ and suppose that $D = 1$. The $n \nmid U_n$ for all $n > 1$. Moreover, if $n > 1$ and $z(n)$ exists, then $z(n) \nmid n$ and $n \nmid z(n)$.*

Theorem 2.8 shows that when $U(P,Q)$ is degenerate and it is not the case that $D = 0$ and $PQ \neq 0$, then we obtain significantly smaller upper bounds for $z(n)$ when $z(n)$ exists than those given in Theorems 2.3 and 2.5. Specifically, we show that for these cases, either $z(n) \leq 1 + \lceil \log_2 n \rceil$ when $z(n)$ exists or $z(n) \leq 6$ for all $n \geq 1$.

Theorem 2.8. *Let $U(P,Q)$ be a degenerate sequence for which it is not the case that $D = 0$ and $PQ \neq 0$. Let α and β be the characteristic roots of $U(P,Q)$. Then the following hold:*

(i) *Suppose that $P = Q = 0$. Then $U_n = 0$ for $n \geq 2$ and $z(n) = 2$ for $n \geq 2$.*

(ii) *Suppose that $P \neq 0$ and $Q = 0$. Then $U_n = P^{n-1}$ for $n \geq 1$. Let P have the prime power factorization*

$$P = \prod_{i=1}^{s} q_i^{\ell_i},$$

where $q_1 < q_2 < \cdots < q_s$ are distinct primes. Then $z(n)$ exists if and only if $\mathrm{rad}(n) \mid P$. *Suppose that $z(n)$ exists and*

$$n = \prod_{i=1}^{s} q_i^{m_i},$$

where $m_i \geq 0$ for $i = 1, \ldots, s$. Then

$$z(n) = \max_{1 \leq i \leq s} \left(\left\lceil \frac{m_i}{\ell_i} \right\rceil + 1 \right) \leq 1 + \lceil \log_2 n \rceil. \tag{2.4}$$

(iii) *Suppose that $\alpha/\beta = -1$. Then $P = 0$ and $Q = N$ for some nonzero integer N. Moreover, $U_2 = 0$ and $z(n) = 2$ for $n \geq 2$.*

(iv) *Suppose that α/β is a primitive cube root of unity. Then $P = N$ and $Q = N^2$ for some nonzero integer N. Moreover, $U_3 = 0$ and $z(n) \leq 3$ for $n \geq 1$.*

(v) *Suppose that α/β is a primitive fourth root of unity. Then $P = 2N$ and $Q = 2N^2$ for some nonzero integer N. Moreover, $U_4 = 0$ and $z(n) \leq 4$ for $n \geq 1$.*

(vi) *Suppose that α/β is a primitive sixth root of unity. Then $P = 3N$ and $Q = 3N^2$ for some nonzero integer N. Moreover, $z(n) \leq 6$ for $n \geq 1$.*

Proof. Parts (i) and (iii)–(vi) follow immediately from parts (i) and (iv)–(vii) of Theorem 1.2. We now prove part (ii). By part (ii) of Theorem 1.2, $U_n = P^{n-1}$ for $n \geq 1$. It is now clear that $z(n)$ exists if and only if $\mathrm{rad}(n) \mid P$. Suppose that $z(n)$ exists. We note that $n \mid U_k = P^{k-1}$ if and only if

$$\ell_i(k-1) \geq m_i \quad \text{for } i = 1, \ldots, s, \tag{2.5}$$

or equivalently,

$$k - 1 \geq \left\lceil \frac{m_i}{\ell_i} \right\rceil \quad \text{for } i = 1, \ldots, s. \tag{2.6}$$

By definition, $z(n)$ is the least k such that (2.6) is satisfied. It is now easily seen that (2.4) holds. □

3. Auxiliary Results

The following known results will be needed for the proof of the main results from Section 2 that are not already proved.

Proposition 3.1. *Consider the Lucas sequence $U(P, Q)$ and companion Lucas sequence $V(P, Q)$. Let $d = \gcd(P, Q)$. Then the following hold:*

(i) *$U_{2n} = U_n V_n$.*

(ii) *If $m \mid n$, then $U_m \mid U_n$.*

(iii) *Let p be a special prime and let $q = p^k$, where $k \geq 1$. Then*

$$p^k \mid U_n \tag{3.1}$$

for all $n \geq 2k$. In particular,

$$z(p^k) \leq 2k \leq \frac{2}{p} p^k \leq p^k. \tag{3.2}$$

If $q = 2^3$, then

$$z(q) \leq 4 \leq \frac{q}{2}. \tag{3.3}$$

If $p \geq 5$, or both $p = 3$ and $k \geq 2$, or both $p = 2$ and $k \geq 4$, then

$$z(q) \leq \frac{4}{9}q. \tag{3.4}$$

(iv) *Suppose that $p \nmid 2Q$. Then*

$$z(p) \mid p - (D/p), \tag{3.5}$$

where (D/p) is the Legendre symbol and $(D/p) = 0$ if $p \mid D$.

(v) *Suppose that $p \nmid 2QD$. Then*

$$z(p) \mid (p - (D/p))/2 \tag{3.6}$$

if and only if $(Q/p) = 1$.

(vi) *If $P \equiv Q \equiv 1 \pmod 2$, then $z(2) = 3$.*

(vii) *Suppose that $p \nmid Q$ and $p \mid D$. Then $z(p) = p$. Moreover, $z(p) = z(p^2)$ if and only if $p = 2$ and $4 \mid P$ or it is the case that $p = 3$ and $P^2 \equiv Q \pmod 9$.*

(viii) *Suppose that $p \nmid Q$. Then $z(p)$ exists. Let $c \geq 1$ be the largest integer such that $z(p) = z(p^c)$. If $p^c \neq 2$ and $k \geq 1$, then*

$$z(p^k) = p^{\max(k-c,0)}z(p). \tag{3.7}$$

If $p^c = 2$, let $e \geq 2$ be the largest integer such that $z(2^2) = z(2^e)$. Then for $k \geq 2$, we have

$$z(p^k) = p^{\max(k-e,0)+1}z(p). \tag{3.8}$$

Furthermore, $e = 2$ if $P \equiv 2 \pmod 4$ and $e \geq 3$ if $P \equiv Q \equiv 1 \pmod 2$. In particular, if $p \mid D$ and $z(p) \neq z(p^2)$, then $z(p^k) = p^k$ for $k \geq 1$.

(ix) *If $z(n) \mid m$, then $n \mid U_m$.*

(x) *If $\gcd(n, Q) = 1$ and $n \mid U_m$, then $z(n) \mid m$.*

(xi) *If $\gcd(m, n) = 1$ and both $z(m)$ and $z(n)$ exist, then $z(mn)$ exists and*

$$z(mn) \leq \operatorname{lcm}(z(m), z(n)) \leq z(m)z(n). \tag{3.9}$$

(xii) *Suppose that $\gcd(m, n) = \gcd(mn, Q) = 1$. If $z(m)$ and $z(n)$ both exist, then $z(mn)$ exists and*

$$z(mn) = \operatorname{lcm}(z(m), z(n)) \leq z(m)z(n). \tag{3.10}$$

(xiii) *The integer $z(n)$ exists if and only if each prime divisor of n is regular.*

Proof. Parts (i) and (ii) follow from the Binet formulas (1.3)–(1.5) and are also proved in [2, pp. 32–33].

(iii) We note that (3.1) follows by induction. The inequalities in (3.2) follow immediately from (3.1). Now suppose that $q = 2^3$. Then by part (i),

$$U_4 = U_2V_2 = P(P^2 - 2Q) \equiv 0 \pmod 8$$

and $z(2^3) \leq 4$, and (3.3) is established. We now show that (3.4) holds. If $p \geq 5$, or $p = 3$ and $k \geq 2$, or $p = 2$ and $k \geq 5$, it follows easily from (3.2) that (3.4) is satisfied with equality in (3.4) if and only if $p = 3$ and $k = 2$. Now suppose that $p = 2$ and $k = 4$. Then

$$U_6 = U_3V_3 = (P^2 - Q)P(P^2 - 3Q). \tag{3.11}$$

If $Q \equiv 0 \pmod 4$, then $U_6 \equiv 0 \pmod{32}$, and

$$z(2^4) \leq 6 \leq \frac{3}{8}q. \tag{3.12}$$

Next assume that $Q \equiv 2 \pmod 4$. We show that $U_4 \equiv 0 \pmod{16}$, which would then imply that

$$z(2^4) \leq 4 \leq \frac{1}{4}q. \tag{3.13}$$

First suppose that $P \equiv 0 \pmod 4$. Then

$$U_4 = U_2V_2 = P(P^2 - 2Q) \equiv 0 \pmod{16}. \tag{3.14}$$

We now consider the case in which $P \equiv 2 \pmod 4$. Then $P^2 \equiv 2Q \equiv 4 \pmod 8$. Thus, (3.14) is again satisfied. Part (iii) is now established.

Parts (iv) and (v) are proved in [5, pp. 423 and 441].

(vi) This follows by inspection upon noting that $U_1 = 1$, $U_2 = P$, and $U_3 = P^2 - Q$.

(vii) It is proved in [5, pp. 423–424], that if $p \nmid Q$ and $p \mid D$, then $z(p) = p$, while if $p \geq 5$, then $z(p) \neq p^2$. Now suppose that $p = 2$. Then $z(2) = 2$. Since $U_2 = P$, we see that $z(2) = z(2^2)$ if and only if $P \equiv 0 \pmod 4$. Next suppose that $p = 3$. Then $z(3) = 3$. Noting that $U_3 = P^2 - Q$, we see that $z(3) = z(3^2)$ if and only if $P^2 \equiv Q \pmod 9$.

(viii) By our earlier observation, if $p \nmid Q$, then $U(P,Q)$ is purely periodic modulo p and $z(p)$ exists. By Theorem X of [2], both of the equalities (3.7) and (3.8) are satisfied. We now suppose that $p = 2$ and $P \equiv 2 \pmod 4$, $Q \equiv 1 \pmod 2$. Then $z(2) = 2$. Thus,

$$U_4 = U_2V_2 = P(P^2 - 2Q) \equiv 4 \pmod 8,$$

and $e = 2$ in this case. If $P \equiv Q \equiv 1 \pmod 2$ and $p = 2$, then $z(2) = 3$. Then

$$U_6 = U_3V_3 = (P^2 - Q)P(P^2 - 3Q) \equiv 0 \pmod 8,$$

since $P^2 \equiv 1 \pmod 4$ and one of the terms $P^2 - Q$ or $P^2 - 3Q$ is congruent to $2 \pmod 4$, while the other term is congruent to $0 \pmod 4$. Hence, $e \geq 3$ in this case. The last assertion follows from part (vii) and from (3.7) and (3.8).

(ix) This follows from part (ii).

(x) This is proved in [2, pp. 35 and 38].

(xi) Suppose that $z(m)$ and $z(n)$ both exist. Let $L = \operatorname{lcm}(z(m), z(n))$. Then by part (ix), $m \mid U_L$ and $n \mid U_L$. Thus, $mn \mid U_L$, and the inequalities in (3.9) immediately follow.

(xii) Suppose that $z(m)$ and $z(n)$ both exist. As in the proof of part (xi), let $L = \operatorname{lcm}(z(m), z(n))$. Noting that $\gcd(m,n) = 1$, it now follows from parts (ix) and (x) that L is the least positive integer such that $mn \mid U_L$. Thus, (3.10) is satisfied.

(xiii) Let p be an irregular prime. It was shown in Theorem I of [2] and is easily proved by induction that $z(p)$ does not exist. It now follows that if n has an irregular prime divisor, then $z(n)$ does not exist.

Now suppose that each prime divisor of n is regular. Let $n = Tm$, where $T \geq 1$, $m \geq 1$, each prime divisor of T is special, and each prime divisor of m is non-special. Then $\gcd(m,Q) = 1$. By our earlier observation, $U(P,Q)$ is purely periodic modulo m and $z(m)$ exists. By part (iii), if p is a special prime and $p^k \mid\mid T$ (where $p^k \mid\mid T$ if $p^k \mid T$ and $p^{k+1} \nmid T$), then $z(p^k)$ exists. It now follows from part (xi) that $z(n) = z(Tm)$ exists. □

Proposition 3.2. *Let b be a basic element of $U(P,Q)$. Then the following hold:*

(i) $\gcd(b,D) = 1$,

(ii) $z(b) = b$.

Proof. It is clear that if $b = 1$, then both (i) and (ii) hold. We now suppose that $b > 1$. We first consider the case in which $P \equiv 3 \pmod 6$, $Q \equiv \pm 1 \pmod 6$, and $b = 6$. Then

$$D = P^2 - 4Q \equiv \pm 1 \pmod 6.$$

Hence, $\gcd(b, D) = \gcd(6, D) = 1$. Further, we see by inspection that $z(2) = 3$ and $z(3) = 2$, since $U_1 = 1$, $U_2 = P \equiv 3 \pmod 6$, and $U_3 = P^2 - Q \equiv \pm 2 \pmod 6$. Thus, by Proposition 3.1 (xii),

$$z(b) = \operatorname{lcm}(z(2), z(3)) = \operatorname{lcm}(3, 2) = 6 = b.$$

We now consider the remaining case in which $P \equiv \pm 1 \pmod 6$, $Q \equiv -1 \pmod 6$, and $b = 12$. Then

$$D = P^2 - 4Q \equiv 5 \pmod 6.$$

Therefore, $\gcd(b, D) = \gcd(12, D) = 1$. By examination, we first find that $z(2) = 3$ and $z(3) = 4$, since $U_2 = P \equiv \pm 1 \pmod 6$, $U_3 = P^2 - Q \equiv 2 \pmod 6$, and $U_4 = P(P^2 - 2Q) \equiv 3 \pmod 6$. Then by Proposition 3.1 (viii) and (xii), we see that whether $z(4) = z(2) = 3$ or $z(4) = 2z(2) = 6$, we have

$$z(b) = z(12) = \operatorname{lcm}(z(4), z(3)) = \operatorname{lcm}(z(4), 4) = 12 = b.$$

□

4. Proof of the Main Results

Proof of Theorem 2.1. We prove parts (i)–(iii) together. First suppose that condition (i) holds. If $p \mid D$ and $p \mid Q$, then $p \mid P$, which implies that $p \mid d$. Hence, $\gcd(R, Q) = 1$. If $R > 1$, let the prime factorization of R be given by $\prod_{i=1}^{s} p_i^{k_i}$. By Proposition 3.2 (i), $\gcd(b, R) = 1$. It follows from Proposition 3.2 (ii) and Proposition 3.1 (vii) and (viii) that $z(b) = b$ and $z\big(p_i^{k_i}\big) = p_i^{k_i}$ for $i = 1, 2, \ldots, s$. We now see by Proposition 3.1 (xii) that $z(n) = n$.

If $2 \mid \gcd(n, d)$, then it is clear that $z(2) = 2$, since $U_2(P, Q) = P$. Now suppose that $P \equiv Q \equiv 2 \pmod 4$. We observe that $U_1 = 1$, $U_2 = P \equiv 2 \pmod 4$, $U_3 = P^2 - Q \equiv 2 \pmod 4$, and $U_4 = P(P^2 - 2Q) \equiv 0 \pmod 4$. Hence, conditions (i)–(iii) are sufficient for $z(n)$ to be equal to n.

We now show that $z(n) \neq n$ if any of conditions (i), (ii), or (iii) are not satisfied. Suppose that n has a prime factor q such that $q \nmid bD$. Notice that we allow both the possibilities that $\gcd(n, d) = 1$ and $\gcd(n, d) > 1$. By way of contradiction, we assume that $z(n) = n$. Then $z(n) \mid n$. Moreover, by Proposition 3.1 (xiii), n has no irregular prime divisors. It now follows from Theorem 1.1 and Proposition 3.1 (ii) that we can express n as $n = mp$, where $m \mid U_m$, p is a prime such that $p \nmid bD$, and $mp \mid U_{mp}$. Then $\gcd(p, d) = 1$. Moreover, by Proposition 3.1 (xiii), $\gcd(p, Q) = 1$. Suppose that $p^k \mid\mid n$. Then

$$m = p^{k-1} m_1, \tag{4.1}$$

where $\gcd(m_1, p) = 1$. By Proposition 3.1 (x),

$$z(p^k) \mid mp. \tag{4.2}$$

It follows from Proposition 3.1 (iv) and (viii) that

$$z(p^k) = p^i z(p), \tag{4.3}$$

where $i \leq k - 1$ and $\gcd(z(p), p) = 1$. Since $\gcd(z(p), p) = 1$, it follows from (4.1), (4.2), and (4.3) that $z(p^k) \mid m$. Thus, by Proposition 3.1 (ix), $p^k \mid U_m$. From $m_1 \mid m$ and $m \mid U_m$, we observe that $m_1 \mid U_m$. Since $\gcd(m_1, p) = 1$, we see that

$$n = mp = p^k m_1 \mid U_m,$$

and

$$z(n) \leq m < n,$$

which is a contradiction.

Next we suppose that $n = bR$ and one of the conditions (i), (ii), or (iii) does not hold. As stated earlier, $z(b) = b$. By Proposition 3.2 (i), $\gcd(b, D) = 1$. Let

$$n = b \prod_{i=1}^{t} q_i^{\ell_i}, \tag{4.4}$$

where the q_i's are distinct primes and $q_1 q_2 \cdots q_t \mid D$. Then by Proposition 3.1 (iii), (vii), and (viii), $z\big(q_i^{\ell_i}\big) \le q_i^{\ell_i}$ for $i = 1, 2, \ldots, t$.

Moreover, by Proposition 3.1 (xi),

$$z(n) \le \operatorname{lcm}\big(z(b), z\big(q_1^{\ell_1}\big), \ldots, z\big(q_t^{\ell_t}\big)\big) \le z(b) \prod_{i=1}^{t} z\big(q_i^{\ell_i}\big) \le b \prod_{i=1}^{t} q_i^{\ell_i}. \tag{4.5}$$

Hence, $z(n) < n$ if we can find a prime q_i, $i \in \{1, \ldots, t\}$, such that $z\big(q_i^{\ell_i}\big) < q_i^{\ell_i}$. Without loss of generality, we denote this prime power by $q_1^{\ell_1}$ if such a prime power exists.

First suppose that $\gcd(n, d) = 1$ and either it is the case that $q_1 = 2$, $\ell_1 \ge 2$, and $P \equiv 0 \pmod 4$, or $q_1 = 3$, $\ell_1 \ge 2$, and $P^2 \equiv Q \pmod 9$. Then by Proposition 3.1 (vii) and (viii), we see that

$$z\big(q_1^{\ell_1}\big) \le q_1^{\ell_1 - 1} < q_1^{\ell_1}.$$

We suppose from here on in the proof that q_1 is a special prime. Suppose that $q_1^{\ell_1}$ is not equal to 2 or 4. Then by Proposition 3.1 (iii),

$$z\big(q_1^{\ell_1}\big) \le \frac{2}{3} q_1^{\ell_1}.$$

The only remaining cases to consider are the ones for which $q_1^{\ell_1} = 2$ and $n > 2$, or $q_1^{\ell_1} = 4$ and it is not the case that both $P \equiv Q \equiv 2 \pmod 4$ and $n = 4$. We note that $z\big(q_1^{\ell_1}\big) = q_1^{\ell_1}$ in some of these cases, so we will have to modify our argument somewhat.

Suppose that $q_1 = 2$, $\ell_1 = 1$, and $n > 2$. Then

$$n = 2b \prod_{i=2}^{t} q_i^{\ell_i}.$$

Since $n/2 \ge 2$, we see by Proposition 3.1 (iii) that $2 \mid U_{n/2}$. Since $b \mid U_b$ and $q_i^{\ell_i} \mid U_{q_i^{\ell_i}}$ for $i \in \{2, \ldots, t\}$ by Proposition 3.2 (ii) and Proposition 3.1 (iii), (vii), and (viii), we find by Proposition 3.1 (ii) that $(n/2) \mid U_{n/2}$. Noting that $\gcd(2, n/2) = 1$, we obtain that

$$z(n) \le n/2 < n.$$

Finally, suppose that $q_1^{\ell_1} = 4$ and it is not the case that $n = 4$ and $P \equiv Q \equiv 2 \pmod 4$. First suppose that $q_1^{\ell_1} = 4$, $n \ge 4$, and either $P \equiv 0 \pmod 4$ or both $P \equiv 2 \pmod 4$ and $Q \equiv 0 \pmod 4$. If $P \equiv 0 \pmod 4$, then $U_2 = P \equiv 0 \pmod 4$ and $z(4) = 2$, implying that $z(n) < n$. If $P \equiv 2 \pmod 4$ and $Q \equiv 0 \pmod 4$, then $U_3 = P^2 - Q \equiv 0 \pmod 4$, and $z(4) = 3$. Again, we have that $z(n) < n$. Now suppose that $P \equiv Q \equiv 2 \pmod 4$ and $n > 4$. Then $n/4 \ge 2$. Hence, $n/2 \ge 4$, and $4 \mid U_{n/2}$ by Proposition 3.1 (iii). Since $\gcd(n/4, 4) = 1$, we see that

$$(n/4) \mid U_{n/4} \mid U_{n/2},$$

and thus, $n \mid U_{n/2}$. Hence, $z(n) \le n/2 < n$. The proof is now complete. □

Proof of Theorem 2.3. By Proposition 3.1 (xiii), $z(n)$ does not exist if and only if n has an irregular prime divisor. We assume from here on that n has no irregular prime divisor. If $R > 1$, let the prime power factorization of R be given by

$$R = \prod_{i=1}^{s} p_i^{k_i}. \tag{4.6}$$

Let

$$n = 2^{k_0} \prod_{i=1}^{s} p_i^{k_i} \prod_{j=1}^{t} q_j^{\ell_j}, \tag{4.7}$$

where $s \geq 0$, $t \geq 0$, $k_0 > 0$ if and only if both $2 \mid n$ and $2 \nmid D$, and the q_j's are primes such that $q_j \nmid 2D$ for $j = 1, \dots, t$. We suppose that $p_1 < p_2 < \cdots < p_s$ and $q_1 < q_2 < \cdots < q_t$. By convention, if $s = 0$ or $t = 0$, we set the associated product equal to 1. We set $\varepsilon_j = (D/q_j)$ for $j = 1, \dots, t$. We define the function ψ by

$$\psi(n, D) = 3^{\min(k_0,1)} 2^{\max(k_0-1,0)} \Big(\prod_{i=1}^{s} p_i^{k_i} \Big) \big(2^{1-t-\delta} \prod_{j=1}^{t} (q_j - \varepsilon_j) q_j^{\ell_j - 1} \big), \tag{4.8}$$

where $\delta = 1$ if either $t = 0$ or it is the case that $t \geq 1$ and either $k_0 \geq 2$ or $2 \mid D$, and $\delta = 0$ otherwise.

By Proposition 3.1 (xi),

$$z(n) \leq \operatorname{lcm}\big(z(2^{k_0}), z(p_1^{k_1}), \dots z(p_s^{k_s}), z(q_1^{\ell_1}), \dots, z(q_t^{\ell_t})\big). \tag{4.9}$$

We note that $2 \mid D$ if and only if $2 \mid P$. Thus, 2 is a regular prime that does not divide D if and only if $P \equiv Q \equiv 1 \pmod 2$. By Proposition 3.1 (vi), $z(2) = 3$ in this case. By Proposition 3.1 (viii), if $k_0 \geq 1$, then

$$z(2^{k_0}) \mid 3 \cdot 2^{k_0 - 1}. \tag{4.10}$$

Moreover, by Proposition 3.1 (iv) and (viii),

$$z(q_j^{\ell_j}) \mid (q_j - (D/q_j)) q_j^{\ell_j - 1}, \tag{4.11}$$

for $j = 1, 2, \dots, t$. If $p_i \mid D$ and $p_i \nmid d$, then

$$z(p_i^{k_i}) \mid p_i^{k_i} \tag{4.12}$$

by Proposition 3.1 (vii) and (viii), where $1 \leq i \leq s$. If $p_i \mid D$ and $p_i \mid d$, then

$$z(p_i^{k_i}) \leq p_i^{k_i}. \tag{4.13}$$

by Proposition 3.1 (iii). Moreover, $2 \mid q_j - \varepsilon_j$ for $j = 1, 2, \dots, t$. Furthermore, $2 \mid 2^{\max(k_0-1,0)}$ if $k_0 \geq 2$. It thus follows from Proposition 3.1 (xi) that

$$z(n) \leq \operatorname{lcm}\big(z(2^{k_0}), z(p_1^{k_1}), \dots, z(p_s^{k_s}), z(q_1^{\ell_1}), \dots, z(q_t^{\ell_t})\big) \leq \psi(n, D). \tag{4.14}$$

We now show that $\frac{\psi(n,D)}{n} \leq 2$, which implies by (4.14) that $z(n) \leq 2n$. First suppose that $k_0 = 0$. Then by (4.14) and Proposition 3.1 (iv), (vii), and (viii), we have that

$$\begin{aligned}\frac{z(n)}{n} &\le \frac{\psi(n,D)}{n}\\ &\le \frac{p_1^{k_1}}{p_1^{k_1}}\frac{p_2^{k_2}}{p_2^{k_2}}\cdots\frac{p_s^{k_s}}{p_s^{k_s}}\frac{(q_1+1)q_1^{\ell_1-1}}{q_1^{\ell_1}}\frac{(q_2+1)q_2^{\ell_2-1}}{2q_2^{\ell_2}}\cdots\frac{(q_t+1)q_t^{\ell_t-1}}{2q_t^{\ell_t}}\\ &\le \frac{(3+1)3^{\ell_1-1}}{3^{\ell_1}}\frac{(q_2+1)q_2^{\ell_2-1}}{2q_2^{\ell_2}}\cdots\frac{(q_t+1)q_t^{\ell_t-1}}{2q_t^{\ell_t}} \le \frac{4\cdot 3^{\ell_1-1}}{3^{\ell_1}} = \frac{4}{3} < 2, \end{aligned} \tag{4.15}$$

since $q_j \ge 5$ for $j = 2, \ldots, t$, and thus in this case,

$$\frac{(q_j+1)q_j^{\ell_j-1}}{2q_j^{\ell_j}} = \frac{q_j+1}{2q_j} = \frac{1}{2} + \frac{1}{2q_j} \le \frac{3}{5} < 1.$$

Now suppose that $k_0 \ge 1$ and either every odd prime divisor of n divides D or both $q_1 \ge 3$ and $\varepsilon_1 = 1$. Then,

$$\frac{z(n)}{n} \le \frac{\psi(n,D)}{n} = \frac{3\cdot 2^{k_0-1}}{2^{k_0}}\Big(\prod_{i=1}^{s}\frac{p_i^{k_i}}{p_i^{k_i}}\Big) = \frac{3}{2} \quad \text{if } k_0 \ge 1 \text{ and } t = 0, \tag{4.16}$$

and

$$\frac{z(n)}{n} \le \frac{\psi(n,D)}{n} = \frac{3\cdot 2^{k_0-1}}{2^{k_0}}\Big(\prod_{i=1}^{s}\frac{p_i^{k_i}}{p_i^{k_i}}\Big)\frac{(q_1-1)q_1^{\ell_1-1}}{q_1^{\ell_1}}\prod_{j=2}^{t}\frac{(q_j+1)q_j^{\ell_j-1}}{2q_j^{\ell_j}} < \frac{3}{2}\cdot 1\cdot 1 = \frac{3}{2} \tag{4.17}$$

if $k_0 \ge 1$, $t \ge 1$, $q_1 \ge 3$, and $\varepsilon_1 = 1$.

Next we suppose that $k_0 \ge 1$, $q_1 \ge 5$, and $\varepsilon_1 = -1$. Then

$$\frac{z(n)}{n} \le \frac{\psi(n,D)}{n} = \frac{3\cdot 2^{k_0-1}}{2^{k_0}}\Big(\prod_{i=1}^{s}\frac{p_i^{k_i}}{p_i^{k_i}}\Big)\frac{(q_1+1)q_1^{\ell_1-1}}{q_1^{\ell_1}}\prod_{j=2}^{t}\frac{(q_j+1)q_j^{\ell_j-1}}{2q_j^{\ell_j}} \le \frac{3}{2}\cdot 1\cdot\frac{q_1+1}{q_1}. \tag{4.18}$$

If $q_1 = 5$, then $q_1 + 1 = 6$, and $3 \mid \gcd(3\cdot 2^{k_0-1}, 6)$. Hence, it follows from (4.18) that in this case,

$$\frac{z(n)}{n} \le \frac{1}{n}\mathrm{lcm}\big(z(2^{k_0}), z(p_1^{k_1}), \ldots, z(p_s^{k_s}), z(q_1^{\ell_1}), \ldots, z(q_t^{\ell_t})\big) \le \frac{\psi(n,D)}{3n} \le \frac{1}{3}\cdot\frac{3}{2}\cdot 1\cdot\frac{6}{5} = \frac{3}{5}. \tag{4.19}$$

If $q_1 > 5$, then by (4.18),

$$\frac{z(n)}{n} \le \frac{3}{2}\cdot\frac{7+1}{7} = \frac{12}{7}. \tag{4.20}$$

From here on, we assume that $k_0 \ge 1$, $q_1 = 3$, and $\varepsilon_1 = -1$. Then $p_i \ge 5$ for $i = 1, 2, \ldots, s$. Suppose that p_i is a special prime for some i such that $1 \le i \le s$. Then

$$\frac{z_i(p_i^{k_i})}{p_i^{k_i}} \le \frac{2}{5}$$

by inequality (3.2) in the statement of Proposition 3.1 (iii). Hence, by Proposition 3.1 (iii), (iv), (vi), (vii), and (viii),

$$\begin{aligned}\frac{z(n)}{n} &\le \frac{1}{n}\operatorname{lcm}\big(z(2^{k_0}), z(p_1^{k_1}), \dots, z(p_s^{k_s}), z(q_1^{\ell_1}), \dots, z(q_t^{\ell_t})\big)\\ &\le \frac{3\cdot 2^{k_0-1}}{2^{k_0}}\Big(\prod_{i=1}^{s}\frac{z(p_i^{k_i})}{p_i^{k_i}}\Big)\frac{(3+1)3^{\ell_1-1}}{3^{\ell_1}}\prod_{j=2}^{t}\frac{(q_j+1)q_j^{\ell_j-1}}{2q_j^{\ell_j}} \le \frac{3}{2}\cdot\frac{2}{5}\cdot\frac{4}{3} = \frac{4}{5}.\end{aligned} \tag{4.21}$$

Next suppose that $k_0 \ge 2$. Then $\delta = 1$, since $t \ge 1$, and thus

$$\frac{z(n)}{n} \le \frac{\psi(n,D)}{n} \le \frac{3\cdot 2^{k_0-1}}{2^{k_0}}\Big(\prod_{i=1}^{s}\frac{p_i^{k_i}}{p_i^{k_i}}\Big)\frac{(3+1)3^{\ell_1-1}}{2\cdot 3^{\ell_1}}\prod_{j=2}^{t}\frac{(q_j+1)q_j^{\ell_j-1}}{2q_j^{\ell_j}} \le \frac{3}{2}\cdot 1\cdot\frac{2}{3} = 1. \tag{4.22}$$

Now we consider the case in which $k_0 = 1$, $q_1 = 3$, $\varepsilon_1 = -1$, $\ell_1 \ge 2$, and $\gcd(n,d) = 1$. Then $3\cdot 2^{k_0-1} = 3$, $(q_1-\varepsilon_1)q_1^{\ell_1-1} = 4\cdot 3^{\ell_1-1}$, and 3 divides both $3\cdot 2^{k_0-1}$ and $(q_1-\varepsilon_1)q_1^{\ell_1-1}$. We now see that in this case,

$$z(n) \le \operatorname{lcm}\big(z(2^{k_0}), z(p_1^{k_1}), \dots, z(p_s^{k_s}), z(q_1^{\ell_1}), \dots, z(q_t^{\ell_t})\big) \mid \frac{\psi(n,D)}{3}. \tag{4.23}$$

Hence,

$$\frac{z(n)}{n} \le \frac{\psi(n,D)}{3n} = \frac{1\cdot 3}{3\cdot 2}\Big(\prod_{i=1}^{s}\frac{p_i^{k_i}}{p_i^{k_i}}\Big)\frac{(3+1)3^{\ell_1-1}}{3^{\ell_1}}\prod_{j=2}^{t}\frac{(q_j+1)q_j^{\ell_j-1}}{2q_j^{\ell_j}} \le \frac{1}{3}\cdot\frac{3}{2}\cdot 1\cdot\frac{4}{3} = \frac{2}{3}. \tag{4.24}$$

Next we suppose that $\gcd(n,d) = 1$, $k_0 = 1$, $q_1 = 3$, $\varepsilon_1 = -1$, $\ell_1 = 1$, and $t \ge 2$. Then

$$\frac{z(n)}{n} \le \frac{\psi(n,D)}{n} \le \frac{3}{2}\Big(\prod_{i=1}^{s}\frac{p_i^{k_i}}{p_i^{k_i}}\Big)\frac{(3+1)3^{0}}{3}\prod_{j=2}^{t}\frac{(q_j+1)q_j^{\ell_j-1}}{2q_j^{\ell_j}} \le \frac{3}{2}\cdot 1\cdot\frac{4}{3}\frac{(5+1)5^{\ell_j-1}}{2\cdot 5^{\ell_j}} = \frac{6}{5}. \tag{4.25}$$

The only remaining case is that in which $\gcd(n,d) = 1$, $k_0 = 1$, $q_1 = 3$, $\varepsilon_1 = -1$, $\ell_1 = 1$, and $t = 1$. Then

$$n = 2\cdot\Big(\prod_{i=1}^{s}p_i^{k_i}\Big)\cdot 3. \tag{4.26}$$

We note that $p_i \ge 5$ and p_i is not a special prime for $i = 1, \dots, s$. It thus follows from Proposition 3.1 (vii) and (viii) that $z(p_i^{k_i}) = p_i^{k_i}$ for $i \in \{1, \dots, s\}$. By Proposition 3.1 (vi), $z(2) = 3$. Since $3 \nmid D$, we see from Proposition 3.1 (iv) that

$$z(3) \mid 3 - (D/3) = 4.$$

Hence, $z(3) = 2$ or $z(3) = 4$, since $U_1 = 1$. Since each prime divisor of n is regular and non-special, it follows that $\gcd(n,Q) = 1$. Then by Proposition 3.1 (xii),

$$z(n) = \operatorname{lcm}\big(z(2), z(3), z(p_1^{k_1}), \dots, z(p_s^{k_s})\big). \tag{4.27}$$

If $z(3) = 2$, then by (4.27),

$$z(n) = \operatorname{lcm}\big(3, 2, p_1^{k_1}, \dots, p_s^{k_s}\big) = 6p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s} = n. \tag{4.28}$$

If $z(3) = 4$, then again by (4.27), we have

$$z(n) = \operatorname{lcm}\big(3, 4, p_1^{k_1}, \dots, p_s^{k_s}\big) = 12p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s} = 2n \tag{4.29}$$

as desired. Thus, $z(n) \le 2n$ whenever $z(n)$ exists and $z(n) = 2n$ if and only if $\gcd(n, d) = 1$, $k_0 = 1$, $q_1 = 3$, $\varepsilon_1 = -1$, $\ell_1 = 1$, $t = 1$, $z(2) = 3$, and $z(3) = 4$. It now follows that if $z(n)$ exists, then $n \mid z(n)$ if and only if $z(n) = n$ or $z(n) = 2n$.

We now determine exactly when $z(2) = 3$ and $z(3) = 4$. By Proposition 3.1 (vi) and our earlier discussion, $z(2) = 3$ if and only if $P \equiv Q \equiv 1 \pmod 2$. Since $U_2 = P$, $U_3 = P^2 - Q$, and $U_4 = U_2V_2 = P(P^2 - 2Q)$, we see that $z(3) = 2$ if $P \equiv 0 \pmod 3$. Thus, $P \equiv \pm 1 \pmod 3$. If $(P, Q) \equiv (\pm 1, 0) \pmod 3$, then 3 is an irregular prime, and $z(3)$ does not exist. Thus, $Q \equiv \pm 1 \pmod 3$. If $Q \equiv 1 \pmod 3$, then $U_3 \equiv 3$ and $z(3) = 3$. If $(P, Q) \equiv (\pm 1, -1) \pmod 3$, then $U_4 \equiv 0 \pmod 3$ and $z(3) = 4$. It now follows from the Chinese Remainder Theorem that $z(2) = 3$ and $z(3) = 4$ if and only if $P \equiv \pm 1 \pmod 6$ and $Q \equiv -1 \pmod 6$. Thus, $z(n) = 2n$ if and only if $P \equiv \pm 1 \pmod 6$, $Q \equiv -1 \pmod 6$, $\gcd(n, d) = 1$, and $n = 6R$. □

Proof of Corollary 2.4. This follows from the inequalities and equalities (4.15)–(4.25) and (4.28)–(4.29) given in the proof of Theorem 2.3. □

Remark 4.1. The function $\psi(n, D)$ used in the proof of Theorem 2.3 is a generalization of the function $\psi(n, D)$ introduced on page 629 of [1] that was defined when $\gcd(n, 2D) = 1$.

Proof of Theorem 2.5. We first show that the Lucas sequences considered in parts (i)–(ii) and (iv)–(v) are nondegenerate. By Theorem 1.2, the Lucas sequence $U(P, Q)$ is degenerate if and only if $PQD = 0$ or $U_n = 0$ for $n = 2, 3, 4,$ or 6. Noting that $U_2 = P$, $U_3 = P^2 - Q$, $U_4 = U_2V_2 = P(P^2 - 2Q)$, and $U_6 = U_3V_3 = (P^2 - Q)P(P^2 - 3Q)$, we see that $U_2U_3U_4U_6 = 0$ if and only if $P(P^2 - Q)(P^2 - 2Q)(P^2 - 3Q) = 0$. By inspection, we see that none of the Lucas sequences discussed in parts (i)–(ii) and (iv)–(v) are degenerate.

We note that part (iii) follows immediately from Theorem 1.2 (iii). We now prove parts (i) and (ii). It follows from our earlier comments and from Proposition 3.1 (iii), (vii), and (viii) that if $p \mid D$, then $z(p^k)$ exists and $z(p^k) \le p^k$ for $k \ge 1$. We now note that it suffices to show that $z(q) < q$ when q is a prime such that $q \nmid D$ and $z(q)$ exists. If $z(q) < q$, it then follows from (3.7) and (3.8) that $z(q^\ell) < q^\ell$ for $\ell \ge 1$. By Proposition 3.1 (xi), parts (i) and (ii) will then follow.

We now suppose that the hypotheses of part (i) hold. We observe that

$$D = P^2 - 4Q = r^2.$$

Suppose that $p \nmid D$ and $z(p)$ exists. If $p = 2$ and $2 \mid P$, then $2 \mid D$. Moreover, if $p = 2$ and P is odd, then $P^2 \equiv r^2 \equiv 1 \pmod 8$, and $2 \mid Q$. Then 2 is an irregular prime in this case. We can thus assume that $p > 2$. Further, $p \nmid r$, since $p \nmid D$. Then by Proposition 3.1 (iv),

$$z(p) \mid p - (D/p) = p - (r^2/p) = p - 1. \tag{4.30}$$

Thus, $z(p) < p$. Moreover, if $D = 1$, then no prime divides D, and it follows from (4.30) and Proposition 3.1 (xi) that $z(n) < n$ when $n > 1$ has no irregular prime divisors. Therefore, part (i) is established.

Now suppose that the hypotheses of part (ii) are satisfied. We then see that $2 \mid D$ or 2 is an irregular prime. We wish to show that $z(p) < p$ whenever $p \nmid D$ and $z(p)$ exists. We can consequently assume that p is odd. Then

$$(Q/p) = (r^2/p) = 1,$$

since p is a regular prime not dividing D. Then by Proposition 3.1 (v),

$$z(p) \mid (p - (D/p))/2 \le (p + 1)/2 < p. \tag{4.31}$$

Hence, $z(p) < p$, and part (ii) follows.

We now prove parts (iv) and (v). By the hypotheses of parts (iv) and (v), it follows that in both cases, every prime dividing QD is a special prime. Consequently, there are no irregular primes and thus $z(n)$ exists for all $n \geq 1$. Moreover, in both cases, 2 and 3 are special primes and

$$z(2) = z(3) = z(4) = z(6) = z(12) = 2, \tag{4.32}$$

since $12 \mid P = U_2$. Furthermore, since $4 \mid P$ and $16 \mid Q$ in both cases, we have

$$U_3 = P^2 - Q \equiv 0 \pmod{16},$$

and thus,

$$z(8) = z(16) \leq 3. \tag{4.33}$$

It now follows from (4.32), (4.33), and Proposition 3.1 (iii) that if p is a special prime and $p^k \geq 5$, then

$$z(p^k) \leq \frac{4}{9}p^k \tag{4.34}$$

when either of the hypotheses of parts (iv) or (v) are satisfied.

We now suppose that the hypotheses of part (iv) hold. Suppose that $p \nmid D$. Then $p \geq 5$ and p is a non-special prime. Moreover, $p \nmid d_1Q_1$, since otherwise, p would divide both P and Q, which would imply that $p \mid D$. Then

$$(Q/p) = (d_1^2Q_1^2/p) = 1.$$

It now follows from Proposition 3.1 (v) that

$$z(p) \mid (p - (D/p))/2 \leq \frac{p+1}{2} \leq \frac{3}{5}p, \tag{4.35}$$

since

$$\frac{p+1}{p} = 1 + \frac{1}{p} \leq \frac{6}{5}.$$

Thus, by Proposition 3.1 (viii),

$$z(p^k) \leq \frac{3}{5}p^k \tag{4.36}$$

for $k \geq 1$.

Let $m_1 \geq 1$ and $m_2 > 1$ be any integers such that the only prime divisors of m_1 are 2 or 3, and the only prime divisors of m_2 are primes greater than 3. It now follows from (4.32)–(4.36) and Proposition 3.1 (xi) that

$$z(m_1m_2) \leq \frac{3}{5}m_1m_2. \tag{4.37}$$

By (3.2), (3.4), (4.32), and (4.33), we see that

$$z(m_1) = m_1 \quad \text{if } m_1 \in \{1, 2\}, \tag{4.38}$$

$$z(m_1) = \frac{2}{3}m_1 \quad \text{if } m_1 = 3, \tag{4.39}$$

$$z(m_1) = \frac{1}{2}m_1 \quad \text{if } m_1 = 4, \tag{4.40}$$

and

$$z(m_1) \leq \frac{4}{9}m_1 \quad \text{if } m_1 \geq 6. \tag{4.41}$$

Part (iv) now follows.

We finally suppose that the hypotheses of part (v) are satisfied. We first note that it is well-known that if (t, Q_1, P_1) is a primitive Pythagorean triple, then either t or Q_1 is divisible by 4 and $60 \mid tQ_1P_1$. Let p be a prime such that $p \nmid D = (d_2t)^2$. Then $p \geq 7$. Moreover, $p \nmid Q$, since any prime dividing Q is a special prime which must then divide D. Thus,

$$(D/p) = (Q/p) = 1.$$

It then follows from Proposition 3.1 (v) that

$$z(p) \mid \frac{p - (D/p)}{2} = \frac{p-1}{2} < \frac{1}{2}p. \tag{4.42}$$

Therefore, by Proposition 3.1 (viii), we have that

$$z(p^k) < \frac{1}{2}p^k \tag{4.43}$$

for $k \geq 1$.

As in the proof of part (iv), let $m_1 \geq 1$ and $m_2 > 1$ be any integers such that the only prime divisors of m_1 are 2 or 3, and the only primes dividing m_2 are those which are greater than 3. It follows from (4.32)–(4.34), (4.42)–(4.43), and Proposition 3.1 (xi) that

$$z(m_1m_2) < \frac{1}{2}m_1m_2. \tag{4.44}$$

We note that the equations (4.38)–(4.41) follow from the hypotheses of part (v) as well as from the hypotheses of part (iv). Making use of (4.38)–(4.41), we see that part (v) holds. □

Proof of Corollary 2.7. It follows from Theorem 1.1 and was earlier proved in Theorem 8 (iii) of [9] that if $D = 1$, then $n \nmid U_n$ for any $n > 1$. If $z(n) \mid n$, then it follows from Proposition 3.1 (ix) that $n \mid U_n$. Hence, $z(n) \nmid n$ for $n > 1$. It further follows from Theorem 2.5 (i) that if $z(n)$ exists, then $z(n) < n$ for $n > 1$. □

5. Concluding Remarks

Below are some corrections for the paper [6].

1. On the bottom of page 348 and the top of page 349 in the proofs of Cases 1 and 2 of the "only if" part of the proof of Theorem 1.1, the author assumes that if $n \mid F_n$ and $n > 1$, then n is of the form $12^a \cdot 5^k m$, where $a + k \geq 1$ and $\gcd(5 \cdot 12, m) = 1$. However, this is incorrect as seen from Theorem 1.1 of our paper and from the sequence A023172 of [7] which lists the initial integers n for which $n \mid F_n$. In particular, 24, 36, 48, 72, 96, 108, and 120 are terms in the sequence A023172, and none of these terms are of the form $12^a \cdot 5^k m$. The correct statement is that if $n \mid F_n$ and $n > 1$, then n is of the form $12^a \cdot 5^k \cdot 2^b \cdot 3^c m$, where $a = 0$ or 1, $a + k \geq 1$, $b \geq 0$, $c \geq 0$, and $\gcd(5 \cdot 12, m) = 1$. This follows from Theorem 1.1 in our paper, which is due to Chris Smyth.

2. In the proof of Case 2 on the top of page 349, the author states that if $n \mid F_n$ and $n = 12^a \cdot 5^k m = 12^a \cdot 5^k qt$, where $\gcd(5 \cdot 12, m) = 1$ and q is a prime factor of m, then $n \mid F_{12^a \cdot 5^k t}$.

However, this is not necessarily true. R. D. Carmichael [2] proved that if $n > 12$, then F_n has a primitive prime factor p, which implies that $z(p) = n$. Let $n = 12^2 \cdot qt$, where q is a prime such that $z(q) = 12^2 = 144$ and t is a prime such that $z(t) = q$. In fact, by the table in [4], we can let $q = 10749957121$. Since $q > 12$, there exists such a prime t. Note that $t \neq q$, since $z(t) = q > 12^2$ and $z(q) = 12^2$. Then $n \mid F_n$ by Theorem 1.1 in our paper. However, then $n \nmid F_{12^2t}$. Note that $n \mid F_{12^2t}$ only if $t \mid F_{12^2t}$. Moreover, $t \mid F_{12^2t}$ if and only if $z(t) = q \mid 12^2t$. However, $q \nmid 12^2$ and $q \nmid t$, so n does not divide F_{12^2t}.

3. Let $\nu_5(n)$ denote the 5-adic valuation of n, that is $\nu_5 = k$ if $5^k \mid n$, but $5^{k+1} \nmid n$. In Proposition 4.3 on page 350 of [6], the author states, "Let a and b be positive integers. If $\nu_5(a) \neq \nu_5(b)$, then the equation $z(n) = an/b$ has no solution in positive integers n." This is incorrect as shown in examples (a) and (b) below:

(a) Let $n = 11$. Then $z(11) = 10$. In this case, the equation $z(n) = 10n/11$ has a solution in positive integers, namely $n = 11$. Note that $\nu_5(10) = 1$, while $\nu_5(11) = 0$.

(b) Let $n = 3001$. Then $z(3001) = 25$. In this case, the equation $z(n) = 25n/3001$ has a solution in positive integers, namely $n = 3001$. Note that $\nu_5(25) = 2$, while $\nu_5(3001) = 0$.

6. Acknowledgement

This paper was supported by Project RVO 67985840.

References

[1] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp., **29** (1975), 620–647.

[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math., **15** (1913), 30–70.

[3] R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quart. J. Pure Appl. Math., **48** (1920), 343–372.

[4] R. Knott, *Fibonacci numbers and the golden section. The first 300 Fibonacci numbers, factored*, http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/Fibonacci/fibtable.html.

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

[6] D. Marques, *Fixed points of the order of appearance in the Fibonacci sequence*, The Fibonacci Quarterly, **50.4** (2012), 346–351.

[7] OEIS Foundation Inc. (2011), The On-Line Encyclopedia of Integer Sequences, http://oeis.org.

[8] C. Smyth, *The terms in Lucas sequences divisible by their indices*, J. Integer Seq., **13.2** (2010), Article 10.2.4, 18 pp.

[9] L. Somer, *Divisibility of terms in Lucas sequences by their subscripts*, In Applications of Fibonacci Numbers, Vol. 5 (Eds. G. E. Bergun, A. N. Philippou, and A. F. Horadam), Kluwer Acad. Publ., Dordrecht, 1993, 515–525.

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

MSC2010: 11B39, 11A41, 11A51

Department of Mathematics, Catholic University of America, Washington, DC 20064
E-mail address: somer@cua.edu

Institute of Mathematics, Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republic
E-mail address: krizek@math.cas.cz