Some Arithmetic Properties of Certain Sequences

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

H. C. Williams\textsuperscript{1}
Department of Mathematics and Statistics
University of Calgary
2500 University Drive NW
Calgary, AB T2N 1N4
Canada
williams@math.ucalgary.ca

Abstract

In an earlier paper it was argued that two sequences, denoted by \{U_n\} and \{W_n\}, constitute the sextic analogues of the well-known Lucas sequences \{u_n\} and \{v_n\}. While a number of the properties of \{U_n\} and \{W_n\} were presented, several arithmetic properties of these sequences were only mentioned in passing. In this paper we discuss the derived sequences \{D_n\} and \{E_n\}, where \(D_n = \gcd(W_n - 6R^n, U_n)\) and \(E_n = \gcd(W_n, U_n)\), in greater detail and show that they possess many number theoretic properties analogous to those of \{u_n\} and \{v_n\}, respectively.

\textsuperscript{1}The second author is supported by NSERC of Canada.
1 Introduction

Let \( p, q \in \mathbb{Z} \) be relatively prime and \( \alpha, \beta \) be the zeros of

\[ x^2 - px + q \]

with discriminant \( \delta = (\alpha - \beta)^2 = p^2 - 4q \). The well-known Lucas sequences \( \{u_n\} \) and \( \{v_n\} \) are defined by

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

These sequences possess many interesting properties and have found applications in primality testing, integer factorization, solution of quadratic and cubic congruences, and cryptography (see [4]). We note here that both sequences are linear recurrence sequences of order 2 and that \( u_n, v_n \in \mathbb{Z} \) whenever \( n \geq 0 \).

Lucas’ problem of extending or generalizing his sequences has been well studied and we refer the reader to [2, Chapter 1] and [3, Section 1] for further information on this topic.

One possible extension of the Lucas sequences, which involves cubic instead of quadratic irrationalities, was investigated in [2] (also see Müller, Roettger and Williams [1]). In this case we let \( P, Q, R \in \mathbb{Z} \) be integers such that \( \gcd(P, Q, R) = 1 \) and let \( \alpha, \beta, \gamma \) be the zeros of

\[ h(x) = x^3 - Px^2 + Qx - R, \quad (1) \]

with discriminant

\[ \Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = Q^2P^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2 \neq 0. \]

Roettger’s sequences \( \{c_n\} \) and \( \{w_n\} \) are defined as

\[ c_n = c_n(P, Q, R) = (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)/((\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)) \]

and

\[ w_n = w_n(P, Q, R) = (\alpha^n + \beta^n)(\beta^n + \gamma^n)(\gamma^n + \alpha^n) - 2R^n. \]

Note here that if \( n \geq 0 \), we have \( c_n, w_n \in \mathbb{Z} \) and \( \{c_n\}, \{w_n\} \) are linear recurrence sequences of order 6.

In [2], it is pointed out that the sequences \( \{c_n\} \) and \( \{w_n\} \) have many properties analogous to those of \( \{u_n\} \) and \( \{v_n\} \), respectively. Recently, these sequences were extended further by Roettger, Williams and Guy [3]. If we put \( \gamma_1 = \alpha/\beta, \gamma_2 = \beta/\gamma, \gamma_3 = \gamma/\alpha, \lambda = R \), then we can write

\[ c_n = \lambda^{n-1}(1 - \gamma_1^n)(1 - \gamma_2^n)(1 - \gamma_3^n)/((1 - \gamma_1)(1 - \gamma_2)(1 - \gamma_3)) \]

and

\[ w_n = v_n - 2R^n, \quad \text{where} \]

\[ v_n = \lambda^n(1 + \gamma_1^n)(1 + \gamma_2^n)(1 + \gamma_3^n). \]
One of the most important properties of the Lucas sequence \( \{u_n\} \) when \( n \geq 0 \) is that it is a divisibility sequence. An integer sequence \( \{A_n\} \) is said to be a divisibility sequence if \( A_n \mid A_m \) whenever \( n \mid m \) and \( A_n \neq 0 \). For example, Roettger’s sequence \( \{c_n\} \) \( (n \geq 0) \) is a divisibility sequence. Suppose we define

\[
U_n = \frac{\lambda^{n-1}(1 - \gamma_1^n)(1 - \gamma_2^n)(1 - \gamma_3^n)}{(1 - \gamma_1)(1 - \gamma_2)(1 - \gamma_3)}, \tag{2}
\]

\[
V_n = \lambda^n(1 + \gamma_1^n)(1 + \gamma_2^n)(1 + \gamma_3^n), \tag{3}
\]

where \( \lambda, \gamma_1, \gamma_2, \gamma_3 \in \mathbb{Q} \); \( \gamma_1, \gamma_2, \gamma_3 \neq 1; \gamma_i \neq \gamma_j \) when \( i \neq j \) and \( \gamma_1 \gamma_2 \gamma_3 = 1 \). In [3], it is shown that if \( U_n, V_n \in \mathbb{Z} \) whenever \( n \geq 0 \), \( \{U_n\} \) is a linear recurrence sequence and \( \{U_n\} \) is also a divisibility sequence, then we must have \( \lambda = R \in \mathbb{Z} \) and \( \rho_i = R(\gamma_i + 1/\gamma_i) \) \( (i = 1, 2, 3) \) must be the zeros of a cubic polynomial

\[
g(x) = x^3 - S_1x^2 + S_2x - S_3, \tag{4}
\]

where

\[
S_3 = RS_1^2 - 2RS_2 - 4R^3 \tag{5}
\]

and \( S_1, S_2 \in \mathbb{Z} \). The six zeros of

\[
G(x) = (x^2 - \rho_1x + R^2)(x^2 - \rho_2x + R^2)(x^2 - \rho_3x + R^2)
= x^6 - S_1x^5 + (S_2 + 3R^2)x^4 - (S_3 + 2R^2S_1)x^3 + R^2(S_2 + 3R^2)x^2 - R^4S_1x + R^6
\]

are \( R\gamma_i, R/\gamma_i \) \( (i = 1, 2, 3) \). If we define \( W_n = V_n - 2R^n \), then both \( \{U_n\} \) and \( \{W_n\} \) are linear recurrence sequences with characteristic polynomial \( G(x) \). Also, \( U_0 = 0, U_1 = 1, U_2 = S_1 + 2R, U_3 = S_1^2 + RS_1 - S_2 - 3R^2, W_0 = 6, W_1 = S_1, W_2 = S_1^2 - 2S_2 - 6R^2, W_3 = S_1^3 - 3S_1S_2 + 3RS_1^2 - 6RS_2 - 3R^2S_1 - 12R^3 \). Furthermore, we have \( U_{-n} = -U_n/R^{2n} \), \( W_{-n} = W_n/R^{2n} \); hence, \( U_n, W_n \in \mathbb{Z} \) when \( n \geq 0 \). It is also the case that \( \{U_n\} \) is a divisibility sequence.

It is shown in [3] that if

\[
S_1 = PQ - 3R, \quad S_2 = P^3R + Q^3 - 5PQR + 3R^2, \tag{6}
\]

then \( U_n(S_1, S_2, R) = c_n(P, Q, R), W_n(S_1, S_2, R) = w_n(P, Q, R) \). If, in the expression (2), we define

\[
\Delta = \lambda^2(1 - \gamma_1)^2(1 - \gamma_2)^2(1 - \gamma_3)^2
= R^2(\gamma_1 + \gamma_2 + \gamma_3 - 1/\gamma_1 - 1/\gamma_2 - 1/\gamma_3)^2, \tag{7}
\]

we find that

\[
\Delta = S_1^2 - 4S_2 + 4RS_1 - 12R^2, \tag{8}
\]
but this is the same as $Q^2P^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2$, the discriminant of $h(x)$, when $S_1$ and $S_2$ are given by (6). If $d$ denotes the discriminant of $g(x)$, then, as shown in [3], we have $d = \Delta \Gamma$, where

$$
\Gamma = R^4(\gamma_1 - \gamma_2)^2(\gamma_2 - \gamma_3)^2(\gamma_3 - \gamma_1)^2
$$

(9)

$$
= S_2^2 + 10RS_1S_2 - 4RS_1^3 - 11R^2S_1^2 + 12R^3S_1 + 24R^2S_2 + 36R^4.
$$

(10)

The discriminant $D$ of $G(x)$ is given by $D = Ed^2R^2$, where

$$
E = R^2\Delta(S_1 + 2R)^2 = (\rho_1 - 4R^2)(\rho_2 - 4R^2)(\rho_3 - 4R^2).
$$

If $S_1$ and $S_2$ are given by (6), then

$$
\Gamma = (RP^3 - Q^3)^2.
$$

(11)

We remark that the condition analogous to $\gcd(P, Q, R) = 1$ for Roettger’s sequences is $\gcd(S_1, S_2, R) = 1$ for the more general $\{W_n\}$ and $\{U_n\}$ sequences.

The duplication formulas are

$$
2W_{2n} = W_n^2 + \Delta U_n^2 - 4R^nW_n, \quad U_{2n} = U_n(W_n + 2R^n)
$$

(12)

and the triplication formulas are

$$
4W_{3n} = 3\Delta U_n^2(W_n + 2R^n) + W_n^2(W_n - 6R^n) + 24R^{2n},
$$

(13)

$$
4U_{3n} = U_n(3W_n^2 + \Delta U_n^2).
$$

(14)

Since $\{U_n\}$ is a divisibility sequence, we must have $U_{3n}/U_n \in \mathbb{Z}$ ($n \geq 0$) and by (14), this means that $4 \mid W_n^2 - \Delta U_n^2$. Thus, if $2 \mid U_n$, then $2 \mid W_n$ and we have proved Proposition 1.

**Proposition 1.** *If $n \geq 0$, then $2 \mid \gcd(W_n, U_n)$ if and only if $2 \mid U_n$. *

The general multiplication formulas for $\{W_n\}$ and $\{U_n\}$ are given as [3, (7.7) and (7.8)].

We observe here that in general for a given $S_1, S_2, R \in \mathbb{Z}$ there do not always exist, $P, Q \in \mathbb{Z}$ such that (6) holds. As a simple example consider $S_1 = -1, S_2 = -4, \text{ and } R = 1$; it is not possible to find integers $P, Q$ such that $PQ = 2$ and $P^3 + Q^3 = 3$. Thus, the sequences $\{W_n(S_1, S_2, R)\}, \{U_n(S_1, S_2, R)\}$ represent a non-trivial extension of Roettger’s sequences $\{w_n\}$ and $\{c_n\}$.

In [3] it is mentioned that if we define

$$
D_n = \gcd(W_n - 6R^n, U_n) \quad \text{and} \quad E_n = \gcd(W_n, U_n),
$$

then the sequences $\{D_n\}$ and $\{E_n\}$ possess many number theoretic properties in common with $\{w_n\}$ and $\{v_n\}$, respectively. Indeed, some of these properties were presented in [3] without proof. The purpose of this paper is to supply these proofs or sketches thereof and to develop some new results concerning $\{D_n\}$ and $\{E_n\}$.
2 Some properties of \( \{D_n\} \)

In this section we will produce some results concerning \( \{D_n\} \) that are similar to those possessed by \( \{u_n\} \). We begin with two simple propositions that easily follow from Lemma 8.1 of [3] and results immediately following that lemma.

**Proposition 2.** If \( \gcd(S_1, S_2, R) = 1 \), then for \( n \geq 0 \) we have

\[
\gcd(D_n, R) | 2.
\]

**Proposition 3.** If \( \gcd(S_1, S_2, R) = 1 \), then for any \( n \geq 0 \), we must have \( 4 \nmid D_n \) whenever \( 2 \mid R \).

In the sequel we will assume that \( S_1, S_2, R \) have been selected such that \( \gcd(S_1, S_2, R) = 1 \).

If we define

\[
F_n = \begin{cases} 
\Delta U^2_n, & \text{when} \ 2 \nmid \Delta U_n; \\
\Delta U^2_n/4, & \text{when} \ 2 \mid \Delta U_n
\end{cases}
\]

we see that since \( 4 \mid W_n^2 - \Delta U^2_n \), \( F_n \) must be an integer. If \( M \) is any divisor of \( F_n \) and \( (M, R) = 1 \), then we can use [3, (7.7) and (7.8)] to show that

\[
\begin{align*}
U_{mn}/U_n &\equiv R^{n(m-1)}K_m(W_n/2R^n) \pmod{M}, \quad (15) \\
W_{mn} &\equiv 2R^{mn}L_m(W_n/2R^n) \pmod{M}, \quad (16)
\end{align*}
\]

where the polynomials \( K_m(x) \) and \( L_m(x) \) are respectively defined in [2, §4.3 and §5.1]. Also, from results in [2] it is easy to show that \( L_m(3) = 3 \) and \( K_m(3) = m^3 \). We next establish that like \( \{u_n\} \), \( \{D_n\} \) is a divisibility sequence.

**Theorem 4.** If \( n, m \geq 1 \), then \( D_n | D_{mn} \).

**Proof.** Since \( \{U_n\} \) is a divisibility sequence it suffices to show \( D_n | W_{mn} - 6R^{mn} \). We let \( 2^{\lambda} || D_n \). If \( \lambda = 0 \) or \( \lambda \geq 1 \) and \( 2 \nmid R \), then \( D_n | F_n \). By Proposition 2, we have \( \gcd(D_n, R) = 1 \) and by (16) we get

\[
W_{mn} \equiv 2R^{mn}L_m(W_n/2R^n) \equiv 2R^{mn}L_m(3) \equiv 6R^{mn} \pmod{D_n}.
\]

If \( \lambda = 1 \), then \( \gcd(D_n/2, R) = 1 \) and \( D_n/2 | F_n \); hence,

\[
W_{mn} \equiv 6R^{mn} \pmod{D_n/2}.
\]

Also, since \( 2 \mid U_n \), we have \( 2 \mid U_{mn} \) and \( 2 \mid W_{mn} \) (Proposition 1). It follows that \( W_{mn} \equiv 6R^{mn} \pmod{2} \) and since \( \gcd(2, D_n/2) = 1 \) we get

\[
W_{mn} \equiv 6R^{mn} \pmod{D_n}.
\]

There remains the case of \( \lambda > 1 \) and \( 2 \mid R \), but this is impossible by Proposition 3. \( \square \)
Let $p$ be any prime. We are next able to present the law of repetition for $p$ in $\{D_n\}$. We denote by $\nu_p(x) (x \in \mathbb{Z})$ that value of $\lambda$ such that $p^\lambda \| x$.

**Theorem 5.** Let $p$ be any prime such that $p > 3$ and suppose that $\nu_p(D_n) \geq 1$.

1. If $\nu_p(U_n) > \nu_p(W_n - 6R^n)$, then $\nu_p(D_{pn}) = \nu_p(D_n) + 2$ and $\nu_p(W_{pn} - 6R^{pn}) < \nu_p(U_{pn})$.
2. If $\nu_p(U_n) = \nu_p(W_n - 6R^n)$ and $\nu_p(U_n) > 1$, then $\nu_p(D_{pn}) = \nu_p(D_n) + 2$ and $\nu_p(W_{pn} - 6R^{pn}) < \nu_p(U_{pn})$.
3. If $\nu_p(U_n) < \nu_p(W_n - 6R^n)$, then if $\nu_p(U_n) > 1$, $\nu_p(D_{pn}) = \nu_p(D_n) + 3$.
4. If $\lambda = 1$, then $\nu_p(D_{pn}) \geq 2$.

**Proof.** These results can be established by making use of the techniques of [2, §5.2], together with the polynomial congruence

$$L_p(x) \equiv 3 + p^2(x - 3) + (p^2(p^2 - 1)/12)(x - 3)^2 + (p^2(p^2 - 1)(p^2 - 4)/360)(x - 3)^3 \pmod{(x - 3)^4},$$

which holds for all primes $p \geq 5$. □

When $p = 3$, the law of repetition for 3 in $\{D_n\}$ is given below.

**Theorem 6.** Let $\nu_3(D_n) \geq 1$.

1. If $\nu_3(U_n) \geq \nu_3(W_n - 6R^n) > 1$, then $\nu_3(D_{3n}) = \nu_3(D_n) + 2$.
2. If $\nu_3(U_n) \geq \nu_3(W_n - 6R^n) = 1$, then $\nu_3(D_{3n}) \geq \nu_3(D_n) + 2$.
3. If $\nu_3(U_n) < \nu_3(W_n - 6R^n)$, then

$$\nu_3(D_{3n}) = \nu_3(D_n) + 3 \text{ when } \nu_3(D_n) > 1$$

or

$$\nu_3(D_{3n}) \geq \nu_3(D_n) + 3 \text{ when } \nu_3(D_n) = 1.$$  □

Proof. These results can be easily proved by making use of the the triplication formulas (13) and (14).

In the case of $p = 2$, there exists a rather complicated law of repetition for $p$ in $\{D_n\}$. We will not provide the complete law here, but we remark that if $\nu_2(D_n) > 1$, then the duplication formulas (12) can be used to show that $\nu_2(D_{2n}) \geq \nu_2(D_n) + 1$. The case of $\nu_2(D_n) = 1$, however, is more problematical. Certainly, if $2 \| R$, there is no law of repetition for 2 in $\{D_n\}$ by Proposition 3. Thus, we need only consider the case of $2 \| D_n$ and $2 \nmid R$. In this case, we can use the duplication and triplication formulas to find that if
i) $4 \mid U_n$, $2 \mid W_n - 6R^n$;

ii) $2 \mid U_n$, $2 \mid W_n - 6R^n$, $2 \mid \Delta$;

iii) $2 \mid U_n$, $4 \mid W_n - 6R^n$, $2 \nmid \Delta$;

then $4 \mid D_{3n}$ and $4 \nmid D_{2n}$. In all other cases we have $4 \mid D_{2n}$.

We also have the following companion result to the law of repetition for any odd prime in \{\{D_n\}\}.

Theorem 7. If $p$ is odd and $\nu_p(D_n) \geq 1$, then $\nu_p(D_{mn}) = \nu_p(D_n)$ whenever $p \nmid m$.

Proof. Since $p \neq 2$, we have $p^{2\lambda} \mid F_n$ when $\lambda = \nu_p(D_n)$, $\gcd(p, R) = 1$ and $W_n \equiv 6R^n$ (mod $p^\lambda$). It follows from (16) that

$$W_{mn} \equiv 2R^{mn}L_m(W_n/2R^n) \equiv 2R^{mn}L_m(3) \equiv 6R^{mn} \pmod{p^\lambda}$$

and by (15) that

$$U_{mn}/U_n \equiv R^{n(m-1)}K_m(3) \equiv m^3R^{n(m-1)} \pmod{p^\lambda}.$$ 

Since $p \nmid m$, it follows that $p^\lambda \mid U_{mn}$ and $p^\lambda \mid W_{mn} - 6R^{mn}$; hence $p^\lambda \mid D_{mn}$.

In the case of $p = 2$, Theorem 7 is not in general true when $\lambda = 1$ and $2 \nmid R$, as we have seen in the above remarks. Of course, we could eliminate this problem if we could impose additional restrictions on $S_1$, $S_2$, $R$ such that none of i), ii) or iii) could occur. If $2 \mid D_n$ and $2 \nmid R$, it is easy to show that cases i), ii) or iii) can occur if and only if $2 \mid \tilde{Q}_n$, where $\tilde{Q}_n = (W_n^2 - \Delta U_n^2)/4$. In a later section we will discuss the parity of $\tilde{Q}_n$ when $2 \mid D_n$. Note that if $4 \mid D_n$, then $2 \mid R$ and $\tilde{Q}_n \equiv 1 \pmod{2}$. If $\lambda > 1$, then we certainly have $2^\lambda \mid D_{mn}$ by Theorem 4 and since $W_n/2R^n \equiv 3 \pmod{2^\lambda-1}$, we get

$$U_{mn}/U_n \equiv m^3R^{n(m-1)} \pmod{2^{\lambda-1}}.$$ 

Thus, if $m$ is odd, then $2 \nmid U_{mn}/U_n$ and $2^\lambda \mid D_{mn}$. Hence Theorem 7 is true when $p = 2$ and $\nu_2(D_n) > 1$.

We conclude this section with a result that is often useful.

Theorem 8. If $m$, $n \geq 1$, then $\gcd(U_{mn}/U_n, D_n) \mid 2m^3$.

Proof. It is easy to show this when $2 \nmid D_n$ because $D_n \mid F_n$ and $\gcd(D_n, R) = 1$. Suppose $2 \mid D_n$; then because $U_n/2 \mid F_n$, we have $D_n/2 \mid F_n$. Also, $\gcd(D_n/2, R) = 1$ by Propositions 2 and 3. Hence, by (15)

$$U_{mn}/U_n \equiv m^3R^{n(m-1)} \pmod{D_n/2}.$$ 

It follows that

$$\gcd(U_{mn}/U_n, D_n/2) \mid m^3$$

and

$$\gcd(U_{mn}/U_n, D_n) \mid 2m^3.$$ 

\[ \square \]
3 The law of apparition for \( m \) in \( \{D_n\} \)

In this section we deal with the problem of when \( m \mid D_n \), when \( m > 1 \). We note that if \( p \) is an odd prime and \( p \mid R \), then \( p \nmid D_n \) \((n \geq 0)\) by Proposition 2. Thus, we may assume that if \( m \) is odd, then \( \gcd(m, R) = 1 \). We define \( \omega = \omega(m) \), if it exists, to be the least positive value of \( n \) such that \( m \mid D_n \). We call \( \omega \) the rank of apparition of \( m \) in \( \{D_n\} \).

We begin by examining the case where \( m \) is a prime \( p \) where \( p \mid d \) and \( p \nmid 2R \).

**Theorem 9.** Let \( p \) be any prime such that \( p \nmid 2R \) and \( p \mid d \). There exists a rank of apparition \( \omega \) of \( p \) in \( \{D_n\} \) and if \( p \mid D_n \) for some \( n \geq 0 \), then \( \omega \mid n \). Also, \( \omega = p \) or \( \omega \mid p \pm 1 \).

**Proof.** By results in the early part of [3, §9], we know that if \( p \mid S_1^2 - 3S_2 \), then \( p \) has a simple rank of apparition \( r_1 \) in \( \{U_n\} \). It is not difficult to show that \( p \mid D_n \) if and only if \( r_1 \mid n \); hence, \( \omega = r_1 \). If \( p \nmid S_1^2 - 3S_2 \), then \( p \) can have two ranks of apparition in \( \{U_n\} \) when \( p \nmid \Delta \) and only one when \( p \mid \Delta \). In either case, it is a simple matter to show that there is a rank of apparition \( \omega \) of \( p \) in \( \{D_n\} \), that \( \omega \neq p \) and that if \( p \mid D_n \), then \( \omega \mid n \).

We next consider the case of \( p = 3 \) and \( 3 \nmid d \).

**Lemma 10.** If \( p = 3 \) and \( 3 \nmid dR \), then \( \omega = \omega(3) \) always exists in \( \{D_n\} \) and if \( 3 \mid D_n \), then \( \omega \mid n \).

**Proof.** We see from [3, Table 2] that there is single rank of apparition \( r \) of \( 3 \) in \( \{U_n\} \). From the duplication formulas we see that if \( 3 \mid U_n \) and \( 3 \nmid W_n \), then \( 3 \mid W_{2n} \) if and only if \( W_n \equiv R^n \) \((\text{mod} \ 3)\) and \( 3 \mid W_{4n} \) if and only if \( W_n \equiv -R^n \) \((\text{mod} \ 3)\). Thus, \( \omega(3) \) always exists and \( \omega = r \), \( 2r \) or \( 4r \). Furthermore, if \( 3 \mid D_n \), then \( \omega \mid n \).

There remains the case of odd \( p \) where \( p \nmid 3dR \). We first need to establish a simple lemma in this case. Here and in the sequel we will denote by \( \mathbb{K}_p \) the splitting field of \( G(x) \in \mathbb{F}_p[x] \).

We can denote the zeros of \( G(x) \in \mathbb{F}_p[x] \) by \( R_{\gamma_i} \) and \( R/\gamma_i \) \((i = 1, 2, 3)\).

**Lemma 11.** If \( p \nmid 2\Delta R \), then \( p \mid D_n \) if and only if \( \gamma_1^n = \gamma_2^n = \gamma_3^n = 1 \) in \( \mathbb{K}_p \).

**Proof.** Certainly, if \( \gamma_1^n = \gamma_2^n = \gamma_3^n = 1 \) in \( \mathbb{K}_p \), then \( p \mid W_n - 6R^n \) and \( p \mid U_n \) by (2) and (3); hence, \( p \mid D_n \). If \( p \nmid D_n \), then since \( p \mid U_n \) and \( p \nmid \Delta \), we may assume without loss of generality that \( \gamma_1^n = 1 \). By [3, (8.4)], we have \( \gamma_2^n - 1 = 0 \) and therefore \( \gamma_3^n = 1/(\gamma_1^n\gamma_2^n) = 1 \).

**Corollary 12.** If \( p \nmid 2\Delta R \) and \( \omega = \omega(p) \) exists for \( p \) in \( \{D_n\} \), then \( p \mid D_n \) if and only if \( \omega \mid n \).

**Proof.** Certainly \( p \mid D_n \) when \( \omega \mid n \) because \( \{D_n\} \) is a divisibility sequence. Suppose next that \( \omega \nmid n \) and \( p \mid D_n \). In this case we have \( n = qw + r \), where \( 0 < r < \omega \). Also, by the lemma we must have \( \gamma_1^n = \gamma_2^n = \gamma_3^n = 1 \), \( \gamma_1^n = \gamma_2^n = \gamma_3^n = 1 \in \mathbb{K}_p \). It follows that \( \gamma_1^n = \gamma_2^n = \gamma_3^n = 1 \) in \( \mathbb{K}_p \) and \( p \mid D_r \), which contradicts the definition of \( \omega \).
We now deal with the case of \( p \nmid 6dR \). Under this condition, we say that \( p \) is an S-prime, Q-prime or I-prime if the splitting field of \( g(x) \in \mathbb{F}_p[x] \) is \( \mathbb{F}_p, \mathbb{F}_{p^2}, \) or \( \mathbb{F}_{p^3} \), respectively. The following theorem follows easily from Lemma 11 and results in [3, §9].

**Theorem 13.** If \( p \) is a prime, \( p \nmid 6dR \) and \( \epsilon = (\Delta/p) \), then

\[
p \mid D_{p-\epsilon} \text{ when } p \text{ is an S-prime},
\]

\[
p \mid D_{p^2-1} \text{ when } p \text{ is a Q-prime},
\]

\[
p \mid D_{p^2+\epsilon p+1} \text{ when } p \text{ is an I-prime}.
\]

We can now assemble the above results in the following theorem.

**Theorem 14.** If \( p \nmid 2R \), there exists a rank of apparition \( \omega (\leq p^2 + p + 1) \) of \( p \) in \( \{D_n\} \) and if \( p \mid D_n \), then \( \omega \mid n \).

In [2, §4.6], S-, Q-, I-primes are discussed with respect to the polynomial \( h(x) \in \mathbb{F}_p[x] \). We next show that if \( S_1, S_2 \) are given by (6), then the splitting fields of \( h(x) \) and \( g(x) \in \mathbb{F}_p[x] \) are the same whenever \( p \nmid 1 \). We let \( \mathbb{L}_1 \) denote the splitting field of \( h(x) \in \mathbb{F}_p[x] \), \( \mathbb{L}_2 \) denote the splitting field of \( g(x) \in \mathbb{F}_p[x] \) and let \( \alpha, \beta, \gamma \) denote the zeros of \( h(x) \) in \( \mathbb{L}_1 \). Since the zeros of \( g(x) \in \mathbb{F}_p[x] \) are given by

\[
\rho_1 = \gamma(\alpha^2 + \beta^2), \quad \rho_2 = \alpha(\beta^2 + \gamma^2), \quad \rho_3 = \beta(\alpha^2 + \gamma^2),
\]

we see that \( \rho_1, \rho_2, \rho_3 \in \mathbb{L}_1 \). If \( \mathbb{L}_1 = \mathbb{F}_p \), then clearly \( \mathbb{L}_2 = \mathbb{F}_p = \mathbb{L}_1 \). If \( \mathbb{L}_1 = \mathbb{F}_{p^2} \), then \( (\Delta/p) = -1 \) and by (11), we get \( (d/p) = (\Gamma \Delta/p) = (\Delta/p) = -1 \); hence, \( \mathbb{L}_2 = \mathbb{F}_{p^2} = \mathbb{L}_1 \). If \( \mathbb{L}_1 = \mathbb{F}_{p^3} \), then \( (d/p) = 1 \) and \( \mathbb{L}_2 \neq \mathbb{F}_{p^2} \). Consider

\[
\rho_1 = \gamma(P^2 - 2Q) - \gamma^3 \in \mathbb{L}_1.
\]

We have

\[
\rho_1^p = \gamma^p(P^2 - 2Q) - \gamma^{3p} = \alpha(P^2 - 2Q) - \alpha^3.
\]

Thus, if \( \rho_1 = \rho_1^p \), then since \( \alpha \neq \gamma \) we must have

\[
\alpha^2 + \alpha \gamma + \gamma^2 = P^2 - 2Q
\]

and \( \beta^2 = \alpha \gamma \) or \( \beta^3 = R \). From (1), we get \( P \beta - Q = 0 \) and \( P^3 \beta - Q^3 = 0 \), which is impossible because \( p \nmid 1 \). Thus, \( \rho_1 \neq \rho_1^p \), and therefore \( \mathbb{L}_2 = \mathbb{F}_{p^3} = \mathbb{L}_1 \).

We have not yet discussed the case of \( p = 2 \). The reason for this is easily seen in [3, Table 1]. We first observe that if \( 2 \mid R, 2 \nmid S_1 \) and \( 2 \mid S_2 \), then \( \omega(2) \) does not exist. Next, if \( 2 \mid S_1 \) and \( 2 \nmid S_2 R \), then \( \omega(2) = 2 \) by definition, but we also have \( 2 \mid D_3 \) and \( \omega(2) \nmid 3 \). Thus to truly have a rank of apparition of 2 in the sense of the results given above we should eliminate the possibility that \( 2 \mid S_1 \) and \( 2 \nmid S_2 R \). When we do this, then by Proposition 2 we have \( \omega(2) \) given by Table 1.
If \( p \nmid 2R \), then \( p \) has a rank of apparition \( \omega \) in \( \{D_n\} \); we now deal with the case when \( m = p^\alpha \) and \( \alpha > 1 \). By the law of repetition we know that \( p^\alpha \mid D_n \) for some \( n > 0 \); hence \( \omega(p^\alpha) \) must exist. If we put \( \omega = \omega(p) \), then since \( p \mid D_{\omega(p^\alpha)} \), we must have \( \omega \mid \omega(p^\alpha) \) by Theorem 14. Put \( s = \omega(p^\alpha)/\omega \) and let \( p^\nu \mid s \), then \( s = p^\nu t \), where \( p \nmid t \). If \( p^\lambda \mid D_{p^\nu \omega} \) and \( \lambda < \alpha \), then \( p^\lambda \mid D_{p^\nu \omega} \) by Theorem 7, which is a contradiction; thus \( \omega(p^\alpha) = p^\nu \omega \). Notice that \( \nu \) is the least positive integer such that \( p^\alpha \mid D_{p^\nu \omega} \).

Next, suppose that \( 2 \nmid m \) and the prime power decomposition of \( m \) is

\[
m = \prod_{i=1}^{k} p_i^{a_i};
\]

we must have

\[
\omega(m) = \text{lcm}(\omega(p_i^{a_i}) : i = 1, 2, \ldots, k).
\]

Thus, if \((m, 2R) = 1\), then \( \omega(m) \) always exists and is given by (17).

## 4 The auxiliary sequences \( \{U_n^*\} \) and \( \{W_n^*\} \)

In order to prove some results concerning \( \{U_n\} \) and \( \{W_n\} \), it is often useful to make use of the auxiliary sequences \( \{U_n^*\} \) and \( \{W_n^*\} \). We put \( \gamma_1^* = \gamma_2/\gamma_1, \gamma_2^* = \gamma_3/\gamma_2, \gamma_3^* = \gamma_1/\gamma_3, R^* = R^2 \) and define

\[
V_n^* = R^{\gamma_1}(1 + \gamma_1^*n)(1 + \gamma_2^*n)(1 + \gamma_3^*n),
\]

\[
U_n^* = R^{\gamma_1-1}(1 - \gamma_1^*n)(1 - \gamma_2^*n)(1 - \gamma_3^*n)/((1 - \gamma_1^*)(1 - \gamma_2^*)(1 - \gamma_3^*)),
\]

\[
W_n^* = V_n^* - 2R^{\gamma_1},
\]

where

\[
\Delta^* = R^{\gamma_2}(1 - \gamma_1^*)^2(1 - \gamma_2^*)^2(1 - \gamma_3^*)^2 = \Gamma \neq 0.
\]

Notice also that

\[
\Gamma^* = R^{\gamma_4^*}(\gamma_1^* - \gamma_2^*)^2(\gamma_2^* - \gamma_3^*)^2(\gamma_3^* - \gamma_1^*)^2
\]

\[
= \Delta^2 U_3^2.
\]

If we put \( \gamma_1^* = \gamma_2^*/\gamma_1^* = 1/\gamma_2^* \), then \( \gamma_1^* = 1/\gamma_2^* \). We also have
\[
\gamma_2^* = \gamma_3^*/\gamma_2^* = 1/\gamma_3^* \quad \gamma_3^* = \gamma_1^*/\gamma_3^* = 1/\gamma_1^*.
\]

hence,

\[
W_n^{**} = R^nW_{3n}, \quad U_n^{**} = R^{n-1}U_{3n}/U_3.
\]

If we put \( \rho_i^* = R^*(\gamma_i^* + 1/\gamma_i^*) \) \((i = 1, 2, 3)\), we get

\[
S_1^* = \rho_1^* + \rho_2^* + \rho_3^* = S_2 - RS_1
\]

(20)
and

\[ S_2^* = \rho_1^* \rho_2^* + \rho_2^* \rho_3^* + \rho_3^* \rho_1^* = RW_3 + R^2 S_1^* \]
\[ = RS_1^3 - 3RS_1 S_2 + 3R^2 S_1 - 5R^2 S_2 - 4R^3 S_1 - 12R^4. \quad (21) \]

Also,

\[ S_3^* = \rho_1^* \rho_2^* \rho_3^* \]
\[ = R^* S_1^2 - 2R^* S_2^* - 4R^3. \]

It follows, then, from the results mentioned in §1, that if we compute the initial values of \( U_n^* \) and \( W_n^* (= V_n^* - 2R^* n) \) by replacing \( R, S_1, S_2 \) by \( R^*, S_1^*, S_2^* \), respectively, then we have both \( \{U_n^*\} \) and \( \{W_n^*\} \) to be linear recurrence sequences of order 6 with characteristic polynomial \( G^*(x) \) and \( \{U_n^*\} \) is a divisibility sequence. It is easy to show as well that \( W_{n+1}^* = W_n^*/R^{2n} \) and \( U_{n+1}^* = -U_n^*/R^{2n} \). We observe further that \( \gcd(S_1^*, S_2^*, S_3^*) = 1 \) if and only if \( \gcd(S_1, S_2, S_3) = 1 \). Thus, the sequences \( \{U_n^*\} \) and \( \{W_n^*\} \) have the same properties as \( \{U_n\} \) and \( \{W_n\} \) with \( R, S_1, S_2 \), replaced by \( R^*, S_1^*, S_2^* \), respectively.

We have shown how to relate the \( \{U_n^*\} \) and \( \{W_n^*\} \) sequences to \( \{U_n\} \) and \( \{W_n\} \) in (19); we can also relate the \( \{U_n^*\} \) and \( \{W_n^*\} \) sequences to \( \{U_n\} \) and \( \{W_n\} \). We define \( \rho_i^{(n)} = R^n(\gamma_i^n + 1/\gamma_i^n) \) \((i = 1, 2, 3)\) and find that

\[ S_1^{(n)} = \rho_1^{(n)} + \rho_2^{(n)} + \rho_3^{(n)} = W_n \]

and

\[ S_2^{(n)} = \rho_1^{(n)} \rho_2^{(n)} + \rho_2^{(n)} \rho_3^{(n)} + \rho_3^{(n)} \rho_1^{(n)} = W_n^* + R^n W_n. \quad (23) \]

Since

\[ \Delta U_n^2 = R^{2n}(1 - \gamma_1^n)^2(1 - \gamma_2^n)^2(1 - \gamma_3^n)^2 \]
\[ = (S_1^{(n)})^2 - 4S_2^{(n)} + 4R^n S_1^{(n)} - 12R^{2n}, \]

we get

\[ \Delta U_n^2 = W_n^2 - 4W_n^* - 12R^{2n} \quad (24) \]

using (22) and (23). This formula, which generalizes (8), is similar to the well-known Lucas function identity

\[ v_n^2 - \delta u_n^2 = 4q^n. \]

Note also that we get

\[ \tilde{Q}_n = W_n^* + 3R^n \]

from (24) and

\[ 4W_n^* = W_n^2 - \Delta U_n^2 - 12R^{2n}, \]

11
the relation connecting \(W_n^*\) to \(W_n\) and \(U_n\). To relate \(U_n^*\) to \(W_n\) and \(U_n\) is somewhat more complicated. From (24), we have

\[
\Delta^*U_{n}^{*2} = W_{n}^{*2} - 4W_{n}^{**2} - 12R^{*2n}.
\]

Hence, from (18), (19), and (24), we get

\[
\Gamma U_{n}^{*2} = ((W_{n}^{*2} - \Delta U_{n}^{*2})/4 - 3R^{2n})^{2} - 4R^{m}W_{3n} - 12R^{4n}.
\]

From (13), we find that

\[
16\Gamma U_{n}^{*2} = W_{n}^{4} - 16R^{m}W_{n}^{3} - 48R^{n}\Delta W_{n}U_{n}^{2} + 72R^{2n}W_{n}^{2} - 72R^{2n}\Delta U_{n}^{2} - 2\Delta W_{n}^{2} U_{n}^{2} + \Delta^{2} U_{n}^{4} - 432R^{4n}, \quad (26)
\]

a formula that generalizes (10).

As promised in §2 we will now investigate the parity of \(\bar{Q}_{n}\) when \(2 \nmid R\) and \(2 \mid D_{n}\). If \(2 \nmid S_{1}\) and \(2 \mid S_{2}\), then by (20) and (21), we have \(2 \nmid S_{1}^{*}\) and \(2 \mid S_{2}^{*}\). It follows that \(2 \mid U_{n}^{*}\) if and only if \(7 \mid n\) and \(2 \mid W_{n}^{*}\) when \(2 \mid D_{n}\). In this case we find from (25) that \(2 \mid \bar{Q}_{n}\) whenever \(2 \mid D_{n}\). If \(2 \nmid S_{1}\) and \(2 \mid S_{2}\), then \(2 \mid S_{1}^{*}\) and \(2 \mid S_{2}^{*}\); hence, \(2 \mid U_{n}^{*}\) if and only if \(2 \mid n\) and we get \(2 \mid W_{n}^{*}\), \(\bar{Q}_{n} \equiv 1 \pmod{2}\) whenever \(2 \mid D_{n}\). If \(2 \nmid S_{1}\) and \(2 \mid S_{2}\), then \(\Delta_{n} = \Gamma \equiv (S_{2} + R S_{1})^{2} \equiv 0 \pmod{4}\) from (10). Since \(4 \mid W_{n}^{*2} - \Delta U_{n}^{*2}\), we get \(2 \mid W_{n}^{*}\) and \(\bar{Q}_{n} \equiv 1 \pmod{2}\).

The only remaining case is \(2 \mid S_{1}\) and \(2 \nmid S_{2}\). In this case \(4 \mid \Delta\) and case (iii) can never occur. We get \(U_{2} \equiv S_{1} + 2 \pmod{4}\) and \(W_{2} - 6R^{2} \equiv 2 \pmod{4}\); thus, we see that cases (i) and (ii) can always occur, depending on the parity of \(S_{1}/2\). In either of these cases, we get \(4 \mid D_{6}\). It follows that if we eliminate the case of \(2 \mid S_{1}\) and \(2 \nmid S_{2} R\), then Theorem 7, will be true for all primes \(p\). Also, we have already seen in §3 that if we eliminate this case, then we have a rank of apparition \(\omega\) of \(2\) in \(\{D_{n}\}\) and \(2 \mid D_{n}\) if and only if \(\omega \mid n\); indeed, if \(\gcd(m, R) = 1\), there always exists a rank of apparition \(\omega\) of \(m\) in \(\{D_{n}\}\) given by (17) such that \(m \mid D_{n}\) if and only if \(\omega \mid n\). We remark here that if \(S_{1}\) and \(S_{2}\) are given by (6), then if \(2 \nmid R\) and \(2 \mid S_{1}\), we must have \(2 \mid S_{2}\). Thus, for the sequences \{\(c_{n}\)\} and \{\(w_{n}\)\} we cannot have the case of \(2 \mid S_{1}\) and \(2 \nmid S_{2} R\).

If \(p\) is an \(I\)-prime and \(p \equiv \epsilon = (\Delta/p) \pmod{3}\), then \(3 \mid p^{2} + \epsilon p + 1\). Since we know in this case that \(p \mid D_{p^{2}+\epsilon p+1}\), it is of some interest to determine a criterion for deciding whether or not \(p \mid D_{(p^{2}+\epsilon p+1)/3}\). Roettger showed for the case of the \{\(c_{n}\)\} and \{\(w_{n}\)\} sequences that \(p \mid D_{(p^{2}+\epsilon p+1)/3} \quad (\epsilon = 1 \text{ in this case if } p \text{ is an I-prime})\) if and only if \(R^{(p-1)/3} \equiv 1 \pmod{p}\) in [2, Theorem 5.14]. In what follows we will extend this result to the \{\(U_{n}\)\} and \{\(W_{n}\)\} sequences. We begin with three preliminary lemmas.

**Lemma 15.** If \(3W_{1}^{2} \equiv -\Delta \pmod{p}\), then \(p\) cannot be an \(I\)-prime.

**Proof.** We have \(W_{1} = S_{1}\) and by (8) we find that

\[
S_{2} \equiv RS_{1}^{2} - 2RS_{1} - 4R^{3} \pmod{p}
\]
and by (5) 
\[ S_3 \equiv -RS_1^2 - 2R^2S_1 + 2R^3 \pmod{p}. \]

Hence 
\[ g(x) \equiv (x + R)(x^2 - (S_1 + R)x + S_1^2 + 2RS_1 - 2R^2) \pmod{p}. \]

Since \( g(x) \) is reducible modulo \( p \), \( p \) cannot be an I-prime.

**Lemma 16.** Let \( p \) be an I-prime and let \( \mathbb{K}_p \) be the splitting field of \( G(x) \in \mathbb{F}[x] \). If \( \zeta \) is a primitive cube root of unity in \( \mathbb{K}_p \), then in \( \mathbb{K}_p \) we can have 
\[ \zeta^k(\gamma_1 + \gamma_2 + \gamma_3) + \zeta^{-k}(\gamma_1^{-1} + \gamma_2^{-1} + \gamma_3^{-1}) = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_1^{-1} + \gamma_2^{-1} + \gamma_3^{-1} \quad (27) \]
if and only if \( 3 | k \).

**Proof.** If \( 3 | k \) it is trivial that (27) must hold. If \( 3 \nmid k \), we first observe that 
\[ \zeta^k + \zeta^{-k} = -1 \]
and we have 
\[ \zeta^k + 1/2 = (\zeta^k - \zeta^{-k})/2, \quad \zeta^{-k} + 1/2 = (\zeta^{-k} - \zeta^k)/2. \]
Thus (27) can hold only if 
\[ \frac{\zeta^k - \zeta^{-k}}{2}(\gamma_1 + \gamma_2 + \gamma_3 - \gamma_1^{-1} - \gamma_2^{-1} - \gamma_3^{-1}) = \frac{3}{2}(\gamma_1 + \gamma_2 + \gamma_3 + \gamma_1^{-1} + \gamma_2^{-1} + \gamma_3^{-1}). \]

On multiplying both sides by \( 2R \) and squaring we find that 
\[ 3W_1^2 \equiv -\Delta \pmod{p}, \]
which by the previous lemma is impossible.

**Lemma 17.** If \( p \) is an I-prime and \( p \mid U_n \), then \( p \mid D_n \).

**Proof.** Since \( p \mid U_n \), we must have \( \gamma_i^n = 1 \) in \( \mathbb{K}_p \) for some \( i \in \{1, 2, 3\} \) by (2). We may assume that \( \gamma_1^n = 1 \). From the proof of [3, Theorem 9.8], we have \( 1 = \gamma_1^{1n} = \gamma_2^{1n} \); hence, \( \gamma_2^n = 1 \) and \( \gamma_3^n = 1/(\gamma_1^n \gamma_2^n) = 1 \). The result now follows by Lemma 11.

We are now able to derive our criterion for when \( p \mid D_{(p^2 + \epsilon p + 1)/3} \).

**Theorem 18.** If \( p \) is an I-prime and \( p \equiv \epsilon \pmod{3} \), then \( p \mid D_{(p^2 + \epsilon p + 1)/3} \) if and only if 
\[ W^*_{(p-\epsilon)/3} \equiv R^{2(p-\epsilon)/3-1}W_1 \pmod{p}. \]

**Proof.** We first note by Lemma 17 and 11 that \( p \mid U_{(p^2 + \epsilon p + 1)/3} \) if and only if \( \gamma_i^{(p^2 + \epsilon p + 1)/3} = 1 \) in \( \mathbb{K}_p \) for all \( i \in \{1, 2, 3\} \). Since \( \gamma_1^{p^2 + \epsilon p + 1} = 1 \) in \( \mathbb{K}_p \), we must have 
\[ \frac{\gamma_1^{p^2 + \epsilon p + 1}}{3} = \zeta^k, \]
where $\zeta$ is a primitive cube root of unity in $\mathbb{K}_p$. It follows that $p \mid D_{(p^2+\epsilon p+1)/3}$ if and only if $3 \mid k$. Now

$$(p^2 + \epsilon p + 1)/3 = (p - \epsilon)(p + 2\epsilon)/3 + 1.$$ 

Hence,

$$\zeta^k = \gamma_1^{(p^2+\epsilon p+1)/3} = \gamma_1^{p+2\epsilon}(p-\epsilon)/3 \gamma_1.$$ 

Since $\gamma_1^p = \gamma_2^{\epsilon}$ (see the proof of [3, Theorem 9.8]), we get

$$\zeta^k = (\gamma_2 \gamma_1^2)^{\epsilon(p-\epsilon)/3} \gamma_1 = \gamma_3^{\epsilon(p-\epsilon)/3} \gamma_1$$

and

$$\gamma_3^{\epsilon(p-\epsilon)/3} = (\zeta^k / \gamma_1)^\epsilon.$$ 

Since $\gamma_3^p = \gamma_1^p / \gamma_3^p = \gamma_2^\epsilon / \gamma_1^\epsilon = \gamma_1^{\epsilon^p}$, we get

$$\gamma_1^{\epsilon^p(p-\epsilon)/3} = (\zeta^{kp}/\gamma_1^p)^\epsilon = \zeta^k / \gamma_2$$

and

$$\gamma_1^{\epsilon(p-\epsilon)/3} = (\zeta^k / \gamma_2)^\epsilon.$$ 

Similarly $\gamma_2^{\epsilon(p-\epsilon)/3} = (\zeta^k / \gamma_3)^\epsilon$. It follows that

$$W_{(p-\epsilon)/3}^* = R^{\epsilon(p-\epsilon)/3}[\zeta^{-k\epsilon}(\gamma_1^\epsilon + \gamma_2^\epsilon + \gamma_3^\epsilon) + \zeta^{k\epsilon}(\gamma_1^{-\epsilon} + \gamma_2^{-\epsilon} + \gamma_3^{-\epsilon})].$$

By Lemma 16, we see that $3 \mid k$ if an only if

$$W_{(p-\epsilon)/3}^* \equiv R^{2(p-\epsilon)/3-1} W_1 \pmod{p}.$$

This criterion can easily be converted to one that involves only the $\{U_n\}$ and $\{W_n\}$ sequences by using (24). At first glance, the criterion of Theorem 18 does not resemble the more elegant rule for $p \mid D_{(p^2+\epsilon p+1)/3}$ when dealing with Roettger’s sequences. In this case we have $\gamma_1 = \alpha / \beta$, $\gamma_2 = \beta / \gamma$, $\gamma_3 = \gamma / \alpha$ and $R = \alpha \beta \gamma$. We can deduce Roettger’s rule in the following corollary of Theorem 18.

**Corollary 19.** Suppose $D_n = \gcd(w_n - 6R^n, c_n)$ and $p$ is an I-prime with respect to $h(x) \in \mathbb{F}_p[x]$, then if $p \equiv 1 \pmod{3}$, we have

$$p \mid D_{(p^2+\epsilon p+1)/3} \iff R^{(p-1)/3} \equiv 1 \pmod{p}.$$ 

14
Proof. Suppose first that \( p \nmid \Gamma \). In this case \( p \) is an I-prime with respect to \( g(x) \in \mathbb{F}_p[x] \) and \( 1 = (d/p) = (\Gamma \Delta/p) = (\Delta/p) = \epsilon \). By Theorem 18 we have \( p \mid D_n^{(\epsilon)/3} \) if and only if \( W_{(n-\epsilon)/3}^{*} \equiv R^{2(\epsilon-\epsilon)\epsilon}/\mathbb{W}_1 \) (mod \( p \)). But in \( \mathbb{K}_p \), we have \( \gamma_1^* = \gamma_2/\gamma_1 = \beta^2/(\alpha \gamma) = \beta^3/R; \) hence,

\[
\gamma_1^{\frac{p-1}{3}} = \beta^{p-1}/R^{(p-1)/3} = (\alpha/\beta)/R^{(p-1)/3} = \gamma_2^{-1}/R^{(p-1)/3}.
\]

Similarly, \( \gamma_2^{\frac{p-1}{3}} = \gamma_3^{-1}/R^{(p-1)/3} \), \( \gamma_3^{\frac{p-1}{3}} = \gamma_1^{-1}/R^{(p-1)/3} \). It follows that

\[
W_{(n-\epsilon)/3}^{*} = R^{(p-1)/3}(R^{(p-1)/3}(\gamma_1 + \gamma_2 + \gamma_3) + R^{-(p-1)/3}(\gamma_1^{-1} + \gamma_2^{-1} + \gamma_3^{-1}))
\]

and by Lemma 16 \( W_{(n-\epsilon)/3}^{*} \equiv R^{2(\epsilon-\epsilon)/3}/\mathbb{W}_1 \) (mod \( p \), if and only if \( R^{(p-1)/3} = 1 \) in \( \mathbb{K}_p \).

Suppose next that \( p \nmid P \). In this case, \( p \) cannot be an I-prime with respect to \( g(x) \). If \( p \nmid P \), then by (11) we have \( R \equiv (Q/P)^3 \) (mod \( p \)) and \( h(Q/P) \equiv 0 \) (mod \( p \)). In this case \( p \) is not an I-prime with respect to \( h(x) \), a contradiction. If \( p \mid P \), then \( p \mid Q \) and \( \alpha^3 = \beta^3 = \gamma^3 = R \) in \( \mathbb{L}_1 \). We have \( \alpha^p = 1 = \beta^p = \gamma^p = R^{(p-1)/3} \) and if \( R^{(p-1)/3} = 1 \) (mod \( p \)), we get \( \alpha^p = \alpha \), and \( p \) is not an I-prime with respect to \( h(x) \in \mathbb{F}_p[x] \), a contradiction. Now \( p \mid D_3 \) and since \( 3 \nmid (p^2 + \epsilon p + 1)/3 \), we have \( p \nmid D_n^{(\epsilon)/3} \). Thus, if \( p \) is an I-prime with respect to \( h(x) \in \mathbb{F}_p[x] \), then \( R^{(p-1)/3} \neq 1 \) (mod \( p \)) and \( p \nmid D_n^{(\epsilon)/3} \).

We conclude this section with the following result concerning

\[
D_n^* = \gcd(W_n^* - 6R^n, U_n).
\]

Theorem 20. If \( p \) is an I-prime and \( p \equiv \epsilon \) (mod 3), then \( p \mid D_n^{(\epsilon)/3} \).

Proof. We observe as above that \( \gamma_1^* = \gamma_2/\gamma_1 \) and

\[
(p^2 + \epsilon p + 1)/3 = (p - \epsilon)(p + 2\epsilon)/3 + 1.
\]

Hence

\[
\gamma_1^{(p^2+\epsilon p+1)/3} = (\gamma_2/\gamma_1)((\gamma_2/\gamma_1)^{p+2\epsilon}(p-\epsilon)/3
\]

in \( \mathbb{K}_p \). Now \( \gamma_2^p = \gamma_3^p = \gamma_2^p \), hence,

\[
(\gamma_2/\gamma_1)^{p+2\epsilon} = (\gamma_2\gamma_3^\epsilon/\gamma_1^2) = \gamma_1^{-3\epsilon}.
\]

It follows that

\[
((\gamma_2/\gamma_1)^{p+2\epsilon}(p-\epsilon)/3 = \gamma_1^{-\epsilon(p-\epsilon)} = \gamma_1/\gamma_2
\]

and

\[
\gamma_1^{(p^2+\epsilon p+1)/3} = 1.
\]

Hence, \( p \mid D_n^{(\epsilon)/3} \). \qed
5 Some properties of \( \{E_n\} \)

We will devote the major portion of this section to the proof that if \( p > 3 \) is a prime and \( p \mid E_n \), then \( p \equiv (\Gamma/p) \pmod{3} \). This generalizes [2, Theorem 6.2]. We observe that by Proposition 2 we have \( \gcd(E_n, R) = 2 \). We now need some preliminary results.

**Lemma 21.** Let \( p \) be any prime such that \( p > 3 \). If \( p \mid E_n \), then in \( \mathbb{K}_p \) we must have

\[
\gamma_i^n = 1, \quad \gamma_j^n + \gamma_j^n + 1 = 0,
\]

where \( i \in \{1, 2, 3\} \) and all \( j \in \{1, 2, 3\} \) such that \( j \neq i \).

**Proof.** If \( p \nmid \Delta \) and \( p \mid U_n \), we may assume with no loss of generality that \( \gamma_1^n = 1 \) in \( \mathbb{K}_p \). If \( p \mid \Delta \) we may assume with no loss of generality that \( \gamma_1 = 1 \) (and \( \gamma_2^n = 1 \)) in \( \mathbb{K}_p \). Now

\[
W_n = V_n - 2R^n = R^n(1 + \gamma_1^n)(1 + \gamma_2^n)(1 + \gamma_3^n) - 2R^n = 2R^n(\gamma_2^n + \gamma_2^n + \gamma_3^n) = 2R^n(1 + \gamma_2^n + 1/\gamma_2^n) = 2R^n(1 + 1/\gamma_3^n + \gamma_3^n),
\]

the latter results following from \( \gamma_1^n = 1 \) and \( \gamma_1^n \gamma_2^n \gamma_3^n = 1 \). Since \( W_n = 0 \) in \( \mathbb{K}_p \), we have \( \gamma_2^n + \gamma_2^n + 1 = \gamma_3^n + \gamma_3^n + 1 = 0 \).

**Lemma 22.** If \( p > 3 \) is a prime, then \( p \mid (E_n, \Gamma) \).

**Proof.** If \( p \nmid \Gamma \), then \( \gamma_1 = \gamma_2, \gamma_2 = \gamma_3 \) or \( \gamma_3 = \gamma_1 \) in \( \mathbb{K}_p \) by (10). If \( p \mid E_n \), then we may assume that \( \gamma_1^n = 1 \) and \( \gamma_2^n + \gamma_2^n + 1 = 0 \) in \( \mathbb{K}_p \) by Lemma 21. If \( \gamma_1 = \gamma_2 \), then \( \gamma_2^n = 1 \), which is impossible because \( p > 3 \). The same is true if \( \gamma_2 = \gamma_3 \) or \( \gamma_3 = \gamma_1 \).

**Lemma 23.** If \( p > 3 \) is a prime, \( p \mid \Delta \) and \( p \mid E_n \), then

\[
p \equiv (\Gamma/p) \pmod{3}.
\]

**Proof.** Since \( p \nmid \Delta \), we may assume with no loss of generality that \( \gamma_1 = 1 \) and therefore \( \gamma_2 \gamma_3 = 1 \) in \( \mathbb{K}_p = \mathbb{F}_p^2 \). Also, by Lemma 21 we may assume that if \( p \mid E_n \), then

\[
\gamma_2^n + \gamma_2^n + 1 = 0
\]

in \( \mathbb{K}_p \). Hence, \( \gamma_2^n = 1 \) and \( \gamma_2^n \neq 1 \) in \( \mathbb{K}_p \). By Lemma 22, \( p \nmid \Gamma \) and

\[
\Gamma^{p-1} = (\gamma_1 - \gamma_2)^{p-1}(\gamma_2 - \gamma_3)^{p-1}(\gamma_3 - \gamma_1)^{p-1} = \frac{(1 - \gamma_2^p)(\gamma_2 - \gamma_3)(\gamma_3 - 1)}{(1 - \gamma_2)(\gamma_2 - \gamma_3)(\gamma_3 - 1)}. \tag{28}
\]

If \( \gamma_2 \in \mathbb{F}_p \), then \( \Gamma^{p-1} = 1 \). Also, from \( \gamma_2^{pn} = \gamma_2^n \), we get \( \gamma_2^{(p-1)n} = 1 \), which, since \( \gamma_2^n \neq 1 \) means that \( 3 \mid p - 1 \) and \( p \equiv (\Gamma/p) \pmod{3} \). If \( \gamma_2 \in \mathbb{F}_p^2 \setminus \mathbb{F}_p \), then \( \gamma_2^n = \gamma_3 \) and \( \gamma_2^{(p-1)n} = -1 \) by (28). Since \( \gamma_2^{pn} = \gamma_3^n = 1/\gamma_2^n \) and \( \gamma_2^{(p+1)n} = 1 \), we see that \( 3 \mid p + 1 \) and \( p \equiv (\Gamma/p) \pmod{3} \). \( \square \)
We now show that if $p$ is an I-prime, then $p \nmid E_n$.

**Theorem 24.** If $p$ is an I-prime, then $p \nmid E_n$.

**Proof.** As noted above we know that if $p$ is an I-prime, then $\gamma_1^p = \gamma_2^p = \gamma_3^p = \gamma_1^\ast$ in $\mathbb{K}_p$.

If $p \mid E_n$, then by Lemma 21, we have $\gamma_1^n = 1$ and $\gamma_2^{2n} + \gamma_2^n + 1 = 0$. Now $\gamma_2^{p^n} = \gamma_3^{p^n} = \gamma_1^n$ and $\gamma_2^{2n} = \gamma_1^n$. Hence,

$$0 = (\gamma_2^{2n} + \gamma_2^n + 1)^{p^2} = 3,$$

which is a contradiction. \(\square\)

We next deal with the case where $p \mid S_1 + 2R$.

**Lemma 25.** If $p \mid d$, $p \nmid S_1 + 2R$ and $p \mid E_n$, then

$$p \equiv (\Gamma/p) \pmod{3}.$$  

**Proof.** Since $p \mid S_1 + 2R$ and $S_1 + 2R = R(\gamma_1 + 1)(\gamma_2 + 1)(\gamma_3 + 1)$, we may assume in $\mathbb{K}_p$ that $\gamma_1 = -1$ and $\gamma_2\gamma_3 = -1$. We get

$$(\gamma_1 + \gamma_2)(\gamma_2 + \gamma_3)(\gamma_3 + \gamma_1) = -(\gamma_2^2 + 1/\gamma_2^2 - 2).$$

Since $S_1 \equiv -2R \pmod{p}$, we get $S_3 \equiv -2RS_2 \pmod{p}$ from (5) and

$$g(x) = (x + 2R)(x^2 + S_2) \in \mathbb{F}_p[x].$$

Since $\rho_1 = R(\gamma_1 + 1/\gamma_1) = -2R$, we get $\rho_2^2 = \rho_3^2 = -S_2$ and $\gamma_2^2 + 1/\gamma_2^2 = \rho_2^2/R^2 - 2 = -S_2/R^2 - 2 \in \mathbb{F}_p$. It follows that $(\gamma_1 + \gamma_2)(\gamma_2 + \gamma_3)(\gamma_3 + \gamma_1) \in \mathbb{F}_p$ and

$$((\gamma_1^2 - \gamma_2^2)(\gamma_2^2 - \gamma_3^2)(\gamma_3^2 - \gamma_1^2))^{p-1} = ((\gamma_1 - \gamma_2)^2(\gamma_2 - \gamma_3)^2(\gamma_3 - \gamma_1)^2)^{p-1} = (\Gamma/p).$$  \(\square\)

As $\gamma_2^2 + 1/\gamma_2^2 \in \mathbb{F}_p$, we must have $\gamma_2^2, 1/\gamma_2^2 \in \mathbb{F}_p$ and $\gamma_2^{p^n} = \gamma_2^2$ or $\gamma_2^{p^n} = \gamma_3^2$. Since $p \nmid d$, we see from (29), that $(\Gamma/p) = 1$, when $\gamma_2^{p^n} = \gamma_2^2$ and $(\Gamma/p) = -1$, when $\gamma_2^{p^n} = \gamma_3^2$.

If $p \mid E_n$, then by Lemma 21, we have $\gamma_i^n = 1$ for some $i \in \{1, 2, 3\}$ and $\gamma_2^{2n} + \gamma_2^n + 1 = 0$ $(i \neq j)$. Since $\gamma_1 = -1$, we see that $i = 1$ and $2 \mid n$. If $(\Gamma/p) = 1$, then $\gamma_2^{np} = \gamma_2^n$ and $\gamma_2^{n(p-1)} = 1$. Since $\gamma_3^{np} = 1$ and $\gamma_2^{np} \neq 1$, we see that $3 \mid p - 1$ and $p \equiv (\Gamma/p) \pmod{3}$. If $(\Gamma/p) = -1$, then $\gamma_2^{np} = \gamma_3^n = 1/\gamma_2^n$ and $\gamma_2^{n(p+1)} = 1$; hence $3 \mid p + 1$ and $p \equiv (\Gamma/p) \pmod{3}$. \(\square\)

We are now ready to prove our main result.

**Theorem 26.** If $p \mid d$, $p \nmid S_1 + 2R$ and $p \mid E_n$, then $p \equiv (\Gamma/p) \pmod{3}$. 

17
Proof. We have already proved this result when \( p \mid d \) and when \( p \mid d \) and \( p \mid S_1 + 2R \). We may assume, then, that \( p \nmid d \) and \( p \nmid S_1 + 2R \). Since \( p \mid E_n \), \( p \) can only be an S-prime or a Q-prime by Theorem 24. If \( p \) is an S-prime, then \( 1 = (d/p) = (\Delta/p)(\Gamma/p) \) and \( (\Gamma/p) = e \); if \( p \) is a Q-prime, then \(-1 = (d/p) = (\Delta/p)(\Gamma/p) \) and \( (\Gamma/p) = -e \). Suppose \( p \) is an S-prime. By results in the proof of [3, Theorem 9.4], we have \( \gamma^p = \gamma_i^p \) \((i = 1, 2, 3) \) in \( \mathbb{K}_p \). By Lemma 21, we get \( \gamma_2^{3n} = 1 \), \( \gamma_2^n \neq 1 \); also, \( \gamma_2^{np} = \gamma_2^{n+p} \) means that \( \gamma_2^{(p+1)n} = 1 \) and \( 3 \mid p - \epsilon \). Similarly, if \( p \) is a Q-prime, then by the results in the proof of [3, Theorem 9.6], we have

\[
\begin{align*}
\gamma_2^p &= \gamma_3^p, \\
\gamma_3^p &= \gamma_3^p, \\
\gamma_4^p &= \gamma_1^p
\end{align*}
\]

in \( \mathbb{K}_p \). In this case we get \( \gamma_2^{p^n} = \gamma_3^{n+p} = (1/\gamma_2)^{p^n} \) and \( \gamma_2^{(p+1)n} = 1 \), \( \gamma_2^{3n} = 1 \) and \( \gamma_2^n \neq 1 \). Hence \( 3 \mid p + \epsilon \) and in either case \( p \equiv (\Gamma/p) \pmod{3} \).

In order to extend Theorem 26, we need to prove the following result.

**Theorem 27.** For any \( n > 0 \), we have \( E_n \mid D_{3n} \).

**Proof.** We can rewrite (13) as

\[
W_{3n} - 6R^{3n} = (W_n - 6R^n)\tilde{Q}_n + \Delta W_n U_n^2, \tag{30}
\]

where \( \tilde{Q}_n = (W_n^2 - \Delta U_n)/4 \). Suppose \( p \) is any odd prime and \( p^\lambda \mid E_n \), where \( \lambda \geq 1 \). Since \( p^\lambda \mid U_n \), we must have \( p^\lambda \mid U_{3n} \). Also, \( p^{2\lambda} \mid \tilde{Q}_n \) and \( p^\lambda \mid W_{3n} - 6R^{3n} \) by (30). Next, suppose that \( 2^\lambda \mid E_n \) and \( \lambda \geq 1 \). We have \( 2 \mid W_n - 6R^n \) and \( 2^{2\lambda-2} \mid \tilde{Q}_n \), \( 2^\lambda \mid U_n \). By (30) we see that \( 2^{2\lambda-1} \mid W_{3n} - 6R^{3n} \) and since \( \lambda \geq 1 \), we have \( 2\lambda - 1 \geq \lambda \) and \( 2^\lambda \mid D_{3n} \). Hence, \( E_n \mid D_{3n} \).

We next prove a result which is analogous to the theorem that states that if \( p \) is an odd prime and \( p \mid v_n \), then \( p \equiv \pm 1 \pmod{2^{v+1}} \), where \( 2^{v} \mid n \). (See [2, Theorem 2.20]).

**Theorem 28.** If \( p \ (> 3) \) is a prime and \( p \mid E_n \), then \( p \equiv (\Gamma/p) \pmod{3^{v+1}} \), where \( 3^v \mid n \).

**Proof.** Since \( p \mid E_n \) and \( p > 3 \), we have \( p \nmid D_{3n} \), as \( p \nmid 6R \). But, by Theorem 27, we know that \( p \nmid D_{3n} \). Thus, if \( \omega \) is the rank of apparition of \( p \) in \( \{D_n\} \), we have \( \omega \mid 3n \) and \( \omega \nmid n \). It follows that \( 3^{v+1} \mid \omega \). Also, since \( p \) is not an I-prime and \( p \nmid 6R \), we must have \( \omega = p \) or \( \omega \mid p^2 - 1 \) by results in §3. Since \( 3 \mid \omega \), we cannot have \( \omega = p \) and therefore \( \omega \mid p^2 - 1 \) and \( 3^{v+1} \mid p^2 - 1 \). Since \( p \nmid \Gamma \), we have \( p^2 - 1 = (p - (\Gamma/p))(p + (\Gamma/p)) \) and \( 3 \mid p - (\Gamma/p) \). Hence \( 3^{v+1} \mid p - (\Gamma/p) \).

\[\Box\]

### 6 Primality tests

In Williams [4], it is shown how Lucas used the properties of \( \{u_n\} \) and \( \{v_n\} \) to develop primality tests for certain families of integers. In this section we will indicate how the properties of \( \{U_n\} \) and \( \{W_n\} \) can be used to produce some primality tests. We begin with a simple result concerning integers of the form \( A3^n + \eta \), where \( \eta^2 = 1 \).
Theorem 29. Let \( N = A3^n + \eta \), where \( 2 \mid A \), \( n \geq 2 \), \( 3 \nmid A \), \( \eta \in \{1, -1\} \) and \( A < 3^n \). If

\[
N \mid U_{N-\eta}/U_{(N-\eta)/3},
\]

then \( N \) is a prime.

Proof. Let \( p \) be any prime divisor of \( N \) and put \( m = (N - \eta)/3 \). We note that \( p \neq 2, 3 \) and by (14)

\[
4U_{3m}/U_m = 3W_m^2 + \Delta U_m^2.
\]

Since \( p \mid U_{3m} \), there must exist some rank of apparition \( r \) of \( p \) in \( \{U_n\} \) such that \( r \mid 3m \). If \( p \mid U_m \) and \( p \mid W_m \), then \( p \mid E_m \) and \( p \equiv (\Gamma/p) \pmod{3^n} \) by Theorem 28. If \( p \nmid U_m \), then \( r \nmid m \) and \( r \nmid 3m \) means that \( 3^n \mid r \). Suppose \( p \nmid dR \). If \( p \) is an S-prime or a Q-prime, then by [3, Corollary 9.5 and Theorem 9.7] we must have \( r \mid p - \epsilon \), where \( \epsilon = (\Delta/p) \); hence \( p \equiv (\Delta/p) \pmod{3^n} \). If \( p \) is an I-prime, then \( r \mid p^2 + \epsilon p + 1 \) by Theorem 9.9 of [3]. Since \( 9 \mid r \), this is impossible. If \( p \mid dR \), then \( r = 3, p \) or divides \( p \pm 1 \). Since \( 9 \mid r \), \( r \neq 3 \) and since \( p \nmid N - \eta \), we cannot have \( r = p \). Thus, in all possible cases, we find that \( p \equiv \pm 1 \pmod{3^n} \) and since \( p \) is odd, we have \( p \geq 2 \cdot 3^n - 1 \). Since \( (2 \cdot 3^n - 1)^2 > N \), \( N \) can only be a prime. \( \square \)

We also note that if \( N \) obeys the conditions in the first line of Theorem 29 and \( N \mid E_{(N-\eta)/3} \), then \( N \) must be a prime.

By extending the results in [2, Chapter 7] it is possible to select the parameters of \( S_1, S_2 \) to make Theorem 29 both a necessary and sufficient test for the primality of \( N \), but this test is much less efficient than one based on the Lucas Functions.

In [3, §9] several primality tests for \( N \) are presented. These tests can be easily proved by using the techniques in [2, Chapter 7], but to be usable they require that we know the complete factorization of

\[
N^2 + N + 1 \quad \text{or} \quad N^2 - N + 1.
\]

Of course, such a circumstance is very unlikely, but we might have a partial factorization of \( N^2 \pm N + 1 \). In what follows we will devise a test for the primality of \( N \) in this case. We first require a simple lemma.

Lemma 30. If \( p \) and \( q \) are distinct primes, \( p > 3 \) and \( p \mid D_{qn} \) and \( p \mid U_{qn}/U_n \), then \( q^{\lambda+1} \mid \omega \), where \( \omega \) is the rank of apparition of \( p \) in \( \{D_n\} \) and \( q^\lambda \parallel n \).

Proof. Suppose \( p \mid D_n \). If \( p \mid U_{qn}/U_n \), then by Theorem 8, we get \( p \mid 2q^3 \), which is impossible. Hence, \( p \nmid D_n \). It follows that since \( p \mid D_{qn} \) (\( \{D_n\} \) is a divisibility sequence), we get \( \omega \mid qn \) and \( \omega \nmid n \), which means that \( q^{\lambda+1} \mid \omega \). \( \square \)

We will also need the easily established technical lemma below.

Lemma 31. If \( x \geq 5 \), then

\[
(x^2 + x + 1)^2 < 2(x^4 - x^2 + 1).
\]
Theorem 32. Let $N$ be a positive integer such that $\gcd(N, 6) = 1$ and put $\eta = 1$ or $-1$. Let $T = N^2 + \eta N + 1$ and suppose that $T' \mid T$, where $\gcd(T', T/T') = 1$ and $T'^2 > 2T$. If $N \mid DT$ and $N \mid U_T/U_{T'/q}$ for all distinct primes $q$ such that $q \mid T'$, then $N$ is a prime.

Proof. Let $p$ be any prime divisor of $N$ and $q$ be any prime divisor of $T'$; then $p \geq 5$ and by Lemma 30 we have $q^\lambda \mid \omega(p)$, where $\omega(p)$ is the rank of apparition of $p$ in $\{D_n\}$ and $q^\lambda \parallel T$. Since $\gcd(T', T/T') = 1$, we have $q^\lambda \parallel T'$; hence, $T' \mid \omega(p)$. Let $\omega$ denote the rank of apparition of $T$ in $\{D_n\}$. We have $\omega \mid T$ and $\omega/q \not\mid T$; hence, $q^\lambda \mid \omega$, where $q^\lambda \parallel T$ and therefore $T' \mid \omega$.

By (17), we have

$$\omega = \text{lcm}(\omega(p_{i^\alpha_i}) : i = 1, 2, \ldots, j),$$

where

$$N = j \prod_{i=1}^{j} p_{i^\alpha_i}$$

is the prime power factorization of $N$. Since $\omega(p_{i^\alpha_i}) = p_{i^\nu_i}^{\omega(p_i)}$, we must have $\nu_i = 1$ because $p_i \nmid T$. We get

$$\omega = \text{lcm}(\omega(p_i) : i = 1, 2, \ldots, j) T' \prod_{i=1}^{j} \frac{\omega(p_i)}{T'}.$$

If we put $T = k\omega$, then

$$T \leq kT' \prod_{i=1}^{j} \frac{\omega(p_i)}{T'} \leq kT' \prod_{i=1}^{j} \frac{p_{i^2} + p_i + 1}{T'}$$

by Theorem 13. Also, since

$$T = N^2 + \eta N + 1 > 2 \prod_{i=1}^{j} \frac{p_{i^2} + p_i + 1}{2},$$

([3, Lemma 9.11], cf. [2, Lemma 7.1]) we get

$$kT' \prod_{i=1}^{j} \frac{p_{i^2} + p_i + 1}{T'} > 2 \prod_{i=1}^{j} \frac{p_{i^2} + p_i + 1}{2}$$

and

$$kT'^{2^j} > 2(T')^j.$$

Hence,

$$k > (T'/2)^{j-1} \geq T'/2 \quad \text{(when } j \geq 2).$$

But since $T/T' = k\omega/T'$, we have $k \leq T/T' < T'/2$, a contradiction; consequently, we can only have $j = 1$ and $N = p^\alpha$. Since $\omega(N) = p^{\nu} \omega(p)$ and $\gcd(p, \omega(N)) = 1$, we get $\omega(p^\alpha) = \omega(p)$. It follows that

$$\omega(N) = \omega(p) \leq p^2 + p + 1.$$
Now $T' | \omega(p)$ means that $\omega(p) \geq T'$ and $p^2 + p + 1 \geq T'$. Since $T'^2 > 2T$, we have for $\alpha \geq 2$

$$(p^2 + p + 1)^2 > 2(p^{2\alpha} + \eta p^\alpha + 1) \geq 2(p^{2\alpha} - p^\alpha + 1) \geq 2(p^4 - p^2 + 1)$$

which is impossible by Lemma 31. Hence we can only have $N = p$. □

Many other primality tests can be devised by making use of the ideas in [2, Chapter 7], but the above should suffice to illustrate the kind of results that can be established.

7 Conclusions

In [3] we showed that the $\{U_n\}$ and $\{W_n\}$ sequences can be considered respectively as the sextic analogues of Lucas’ $\{u_n\}$ and $\{v_n\}$ sequences. In this paper we have produced a number of results that are the number-theoretic analogues of well-known properties of the Lucas functions. Of course, there are many other properties of $\{D_n\}$ and $\{E_n\}$ that are similar to those of the $\{D_n\}$ and $\{E_n\}$ sequences discussed at some length in [2], and these can be proved by using the results presented here and the techniques of [2].

References


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

Received February 5 2015; revised version received May 11 2015; May 29 2015. Published in *Journal of Integer Sequences*, May 30 2015.

Return to *Journal of Integer Sequences* home page.