Ann. Sci. Math. Québec **33** (2009), no 2, 185–224

# A CUBIC EXTENSION OF THE LUCAS FUNCTIONS

SIGUNA MÜLLER, ERIC ROETTGER AND HUGH C. WILLIAMS

*Dedicated to Paulo Ribenboim on the occasion of his 80th birthday.*

RÉSUMÉ. Entre 1876 et 1878, Lucas développa la théorie des fonctions $V_n$ et $U_n$ qui portent aujourd'hui son nom. Il s'intéressa beaucoup aux moyens de montrer la primalité de certains grands nombres premiers à l'aide de ces fonctions, et parvint, en particulier, à prouver que $2^{127}-1$ est un nombre de Mersenne premier. Si $V_n$ et $U_n$ s'expriment en fonction des puissances $n$-ièmes des zéros d'un polynôme quadratique, on trouve à travers les écrits de Lucas des allusions répétées à l'étude de fonctions qui puissent généraliser les fonctions $V_n$ et $U_n$ et s'exprimer à l'aide des puissances $n$-ièmes des racines d'un polynôme cubique.

Dans cet article, nous présentons deux fonctions qui s'expriment simplement à l'aide de certains polynômes symétriques des racines des zéros d'un polynôme de degré 3, et dont les propriétés semblent en accord avec la théorie que Lucas avait envisagée. Ainsi, nous établissons clairement que les aspects combinatoires et arithmétiques de nos fonctions étendent la théorie classique de Lucas, et développons aussi des résultats nouveaux qui illustrent davantage la remarquable analogie entre nos fonctions et les fonctions $V_n$ et $U_n$ de Lucas. Aussi nous mettrons en évidence le fait que, bien que Lucas n'ait probablement jamais développé la théorie que nous exposons ici, les moyens mathématiques étaient néanmoins à sa disposition et à sa portée.

ABSTRACT. From 1876 to 1878, Lucas developed his theory of the functions $V_n$ and $U_n$, which now bear his name. He was particularly interested in how these functions could be employed in proving the primality of certain large integers, and as part of his investigations he succeeded in demonstrating that the Mersenne number $2^{127}-1$ is a prime. The functions $V_n$ and $U_n$ can be expressed in terms of the $n$-th powers of the zeros of a quadratic polynomial, and throughout his writings Lucas speculated about the possible extension of these functions to those which could be expressed in terms of the $n$-th powers of the zeros of a cubic polynomial.

In this paper we discuss a pair of functions that are easily expressed as certain symmetric polynomials of the zeros of a cubic polynomial. We show how their properties seem to underlie the theory that Lucas was seeking. We do this by deriving a number of results which show how the combinatorial and arithmetic aspects of these functions provide an extension of Lucas's theory. Furthermore, we develop many new results, which illustrate the striking analogy between our functions and those of Lucas. We also argue that, while Lucas very likely never developed this theory, it was certainly within his abilities to do so.

Reçu le 29 avril 2009 et, sous forme définitive, le 26 novembre 2009.

# 1. Introduction

The present paper is a condensed version of the results in [Roe09], a 218 page thesis devoted to developing the properties of two functions analogous to the well-known functions of Lucas. As such, much detail has been omitted, including many lengthy proofs. The interested reader can find full details in the original work. In several of Lucas's works concerning the development of the theory of his functions, (see Section 1.2 of [Roe09] for full details), he mentioned the possibility of extending his theory. It seems, however, that he never succeeded in doing this. The main tools employed in our investigation into this problem would have been known to Lucas. For example, he would have needed the fundamental theorem of symmetric polynomials, but he indicated in several places (see, for example, Section 21 of [Luc78]), that he was well aware of this result. We will make a great deal of use of Waring's theorem, but this was described in great detail by Lucas in Chapter XV of [Luc91b]. We will also use the theory of finite fields, but this would have been known (at least the amount that he would need) to Lucas through the second volume of Serret's *Cours d'Algèbre supérieure* [Ser79], with which Lucas was quite familiar (see p. vii of [Luc91b]). To develop our law of repetition, we require a small amount of algebraic number theory to prove Theorem 5.7. Lucas might have been aware of some of this material because he claims in part CLIX of [Luc80] that he was working, together with M. Tastavin, on producing a French translation of the third edition of Dirichlet–Dedekind's *Vorlesungen über die Zahlentheorie*. Unfortunately, this volume never appeared, but the result that we need could easily have been deduced by Lucas, even though his proof might not have been completely rigorous. In the Appendix of [Roe09], we provide an alternate, more elementary proof of Theorem 5.7, which Lucas could have been able to deduce. We also make use of derivatives to establish a certain identity that will be useful in our investigation into the law of repetition, but Lucas often did this himself (see, for example, Section XVII of [Luc78]).

The result of this work is a fairly complete cubic generalization of the theory of the Lucas functions. In the next section we list the most important properties of the Lucas functions. In the succeeding sections we will develop analogues of all of these results in our cubic extension of Lucas's functions.

# 2. Lucas sequences

Given the polynomial $x^2 - Px + Q$, where $P$ and $Q$ are coprime integers, the Lucas functions $U_n$ and $V_n$ are defined by

$$U_n = U_n(P, Q) = (\alpha^n - \beta^n)/(\alpha - \beta)$$

and

$$V_n = V_n(P, Q) = \alpha^n + \beta^n,$$

where $\alpha$ and $\beta$ are the zeros of the given polynomial. Further let

$$\Delta = \delta^2 = (\alpha - \beta)^2 = P^2 - 4Q.$$

### 2.1. Identities

Lucas sequences satisfy many well-known identities, several of which will be mentioned herein. For further information the reader is referred to standard works such as [Wil98] and [Rib89].

For a fixed $m$, both $U_n$ and $V_n$ satisfy the following recurrence relation

$$X_{n+2m} = V_m X_{n+m} - Q^m X_n, \tag{1}$$

where $U_0 = 0$, $U_1 = 1$, $V_0 = 2$ and $V_1 = P$. Further, we have:

$$U_{n+m} = V_m U_n - Q^m U_{n-m}, \tag{2}$$

$$V_{n+m} = V_m V_n - Q^m V_{n-m}, \tag{3}$$

$$2U_{m+n} = V_m U_n + U_m V_n, \tag{4}$$

$$2V_{m+n} = V_m V_n + \Delta U_m U_n, \tag{5}$$

$$2Q^m U_{n-m} = U_n V_m - V_n U_m, \tag{6}$$

$$2Q^m V_{n-m} = V_n V_m - \Delta U_n U_m, \tag{7}$$

$$U_{n+m} = V_n U_m + Q^m U_{n-m}, \tag{8}$$

$$V_{m+n} = \Delta U_n U_m + Q^m V_{n-m}, \tag{9}$$

$$V_n^2 - \Delta U_n^2 = 4Q^n, \tag{10}$$

$$U_{2n} = V_n U_n, \tag{11}$$

$$V_{2n} = V_n^2 - 2Q^n = \Delta U_n^2 + 2Q^n. \tag{12}$$

Furthermore:

$$2^{m-1} U_{mn} = \sum_{i=0}^{\lfloor (m-1)/2 \rfloor} \binom{m}{2i+1} \Delta^i U_n^{2i+1} V_n^{m-2i-1}, \tag{13}$$

$$2^{m-1} V_{mn} = \sum_{i=0}^{\lfloor m/2 \rfloor} \binom{m}{2i} \Delta^i U_n^{2i} V_n^{m-2i}. \tag{14}$$

### 2.2. Arithmetic results

The identities from the previous section may be employed to construct arithmetic results for Lucas sequences. Most of the results provided below were known to Lucas, but some such as Theorems 2.4 and 2.15 were not. As is usual, we denote the greatest common divisor of $a$ and $b$ by $(a, b)$ and the least common multiple of $a$ and $b$ by $[a, b]$. It is well-known that

$$(U_n, V_n) \mid 2, \quad \text{for } n \geq 0, \tag{15}$$

and

$$(U_n, Q) = (V_n, Q) = 1, \quad \text{for } n \geq 1.$$

Furthermore, it is not difficult to show that $\{U_n\}$ is a *divisibility sequence*, *i.e.*,

$$U_m \mid U_n, \quad \text{when } m \mid n.$$

**Definition 2.1.** Given $m \in \mathbb{Z}$, let $\omega$ be the least positive integer, if it exists, such that $m \mid U_\omega$. This value is called the *rank of apparition* of $m$, denoted by $\omega(m)$.

**Theorem 2.2.** *Let $(Q,m) = 1$ and $\omega = \omega(m)$. If $m \mid U_n$ for some $n > 0$, then $\omega \mid n$.*

**Corollary 2.3.** *If $m, n > 0$ and $d = (m,n)$, then*

$$(U_m, U_n) = |U_d|.$$

The following theorem is a result of Carmichael, and may be found as a corollary to Theorem 17 in [Car13].

**Theorem 2.4.** *If $m, n \geq 1$, then*

$$(U_{mn}/U_n, U_n) \mid m.$$

We are often interested in values of $n$ for which a prime $p$ divides $U_n$. It will be assumed that $p \nmid Q$. Notice that if $p \mid Q$, then $p \nmid P$ and

$$U_n \equiv P^{n-1} \pmod{p}.$$

Thus, $p \mid U_0$ and $p \nmid U_n$ for $n \geq 1$. The following theorem provides us with what is called the *law of repetition* for a prime $p$.

**Theorem 2.5.** *If $p$ is a prime and, for $\lambda > 0$, we have $p^\lambda \neq 2$ and $p^\lambda \mid\mid U_n$, then $p^{\lambda+1} \mid\mid U_{pn}$. If $p^\lambda = 2$, then $p^{\lambda+1} \mid U_{pn}$.*

**Definition 2.6.** Let $\epsilon(n)$ be the Jacobi symbol $(\Delta/n)$.

The following theorem is called the *law of apparition* for a prime $p$. Let $\epsilon = \epsilon(p)$ for the remainder of the section.

**Theorem 2.7.** *If $p$ is a prime such that $p \nmid 2Q$, then $V_{p-\epsilon} \equiv 2Q^{(1-\epsilon)/2} \pmod{p}$ and $p \mid U_{p-\epsilon}$, that is, $\omega(p) \mid p - \epsilon$.*

We have similar arithmetic results for $\{V_n\}$; many of these were possibly not known to Lucas, but might have appeared in the subsequent literature (see, for example, [Mül01]). In any event, we make no claims of originality of these results.

It is known that $\{U_n\}$ is a divisibility sequence, but this is not necessarily true for $\{V_n\}$; however, we have the following weaker results provided by the next two theorems.

**Theorem 2.8.** *If $m \mid n$ and $2 \nmid \frac{n}{m}$, then $V_m \mid V_n$.*

**Theorem 2.9.** *If $m \mid n$ and $2 \mid \frac{n}{m}$, then $(V_m, V_n) \mid 2$.*

The rank of apparition has been introduced for $\{U_n\}$, and we might expect to have something similar for $\{V_n\}$. But the situation may exist where $r \nmid V_n$ for every $n \in \mathbb{Z}$, hence the following modified definition for the $\{V_n\}$ case is needed.

**Definition 2.10.** Suppose that $r \mid V_n$, with $n > 0$. Denote by $\rho(r)$ the least positive integer $\rho$ such that $r \mid V_\rho$.

**Theorem 2.11.** *If $r \mid V_n$ for some $n > 0$, then $\rho(r) \mid n$.*

**Theorem 2.12.** *If $2^\mu \mid\mid m$ and $2^\mu \mid\mid n$, then $(V_m, V_n) = |V_{(m,n)}|$.*

**Theorem 2.13.** *If $2^\mu \mid\mid m$ and $2^\nu \mid\mid n$ $(\mu \neq \nu)$, then $(V_m, V_n) \mid 2$.*

The short theorem below, which was known to Lucas, is of interest because it was the fundamental result that he required to establish his test for the primality of Mersenne numbers.

**Theorem 2.14.** *If $p$ is an odd prime and $p \mid V_n$, then $p \equiv \pm 1 \pmod{2^{\nu+1}}$, where $2^\nu \mid\mid n$.*

We know, by Theorem 2.7, that for a prime $p$ where $p \nmid 2\Delta Q$, we have $p \mid U_{p-\epsilon}$. Thus, $U_{p-\epsilon} = U_{\frac{p-\epsilon}{2}} V_{\frac{p-\epsilon}{2}}$ and so $p \mid U_{\frac{p-\epsilon}{2}}$ or $p \mid V_{\frac{p-\epsilon}{2}}$, but not both. The question of which one is divisible by $p$ is answered by the following theorem, called *Euler's criterion* for the Lucas functions. This result was not known to Lucas and was first proved in a more general setting by Lehmer [Leh30].

**Theorem 2.15.** *If $p$ is a prime such that $p \nmid 2\Delta Q$, then*

(a) *$p \mid U_{\frac{p-\epsilon}{2}}$ if and only if $(Q/p) = 1$,*

(b) *$p \mid V_{\frac{p-\epsilon}{2}}$ if and only if $(Q/p) = -1$.*

## 2.3. Primality testing

Lucas's main purpose for his investigation into the sequences now named for him was to find new methods for the discovery of primes. This can be seen in the following result, which Lucas called his fundamental theorem.

**Theorem 2.16.** *Suppose that $N$ is an odd integer. Let $T = T(N) = N + 1$ or $T = T(N) = N - 1$. If $N \mid U_T$, but $N \nmid U_{T/d}$ for all $d$ such that $d < T$ and $d \mid T$, then $N$ is a prime.*

It was Lehmer [Leh27], who realized that this theorem could be rewritten as follows.

**Theorem 2.17.** *Suppose that $N$ is an odd integer. Let $T = T(N) = N + 1$ or $T = T(N) = N - 1$. If $N \mid U_T$, but $N \nmid U_{T/q}$ for each prime divisor $q$ of $T$, then $N$ is a prime.*

We also have the following corollary.

**Corollary 2.18.** *Suppose that $N$ is an odd integer and $T = T(N) = N + 1$ or $T = T(N) = N - 1$. If $N \mid U_T$ and $N \mid U_T/U_{T/q}$ for each prime divisor $q$ of $T$, then $N$ is a prime.*

The following theorem is called the Lucas-Lehmer theorem. Lucas used a result similar to this one to implement a primality test for Mersenne numbers.

**Theorem 2.19.** *If $N = A2^n - 1$, $n \geq 3$, $0 < A < 2^n$, $2 \nmid A$, and the Jacobi symbols $(\Delta/N) = (Q/N) = -1$, then $N$ is a prime if and only if*

$$N \mid V_{\frac{N+1}{2}}(P, Q).$$

**Corollary 2.20.** *Suppose that $A = 1$ and $2 \nmid n$, with $n \geq 3$. Put $Q = -2$ and $P \equiv 2 \pmod{N}$. Then $N$ is a prime if and only if*

$$N \mid V_{\frac{N+1}{2}}(2, -2).$$

Put $S_0 = 4$ and $S_{j+1} = S_j^2 - 2$. Then

$$N \mid V_{\frac{N+1}{2}}(2,-2) \text{ if and only if } N|S_{n-2},$$

as

$$V_{2^j}(2,-2) = 2^{2^{j-1}} S_{j-1}.$$

Thus, if $N$ is a Mersenne number, we have that $N$ is a prime if and only if $N \ |S_{n-2}$. It is this corollary that provides an efficient test for Mersenne primes; for further information see [Leh35].

We conclude this chapter by characterizing all the values of $P$ and $Q$ modulo a prime $p \equiv -1 \pmod 4$ for which $\left(\frac{\Delta}{p}\right) = \left(\frac{Q}{p}\right) = -1$. We use the notation $\bar{\alpha}$ to denote the conjugate of $\alpha$ in $\mathbb{Q}(\sqrt{\Delta})$ and we use $N(\alpha) = \alpha\bar{\alpha}$ to denote the norm of $\alpha$ and $Tr(\alpha) = \alpha + \bar{\alpha}$ to denote the trace of $\alpha$.

**Theorem 2.21.** *Let $p$ be a prime such that $p \equiv -1 \pmod 4$. There exist $P$ and $Q$ such that $\left(\frac{\Delta}{p}\right) = \left(\frac{Q}{p}\right) = -1$ if and only if $Q \equiv N(\lambda)$ and $P \equiv Tr(\lambda) \pmod p$, where $\lambda \in \mathbb{Z}[i]$ and $\left(\frac{N(\lambda)}{p}\right) = -1$.*

## 3. The problem

### 3.1. Introduction

From 1876 until about 1880, Édouard Lucas discovered many properties of his functions. Indeed, it was during this period that he used these properties to develop tests for the primality of large integers. These tests were usually sufficiency tests, which could be used to prove whether a number $N$ of a certain special form is a prime. As Lucas well realized, these tests were quite novel for their time, because instead of having to try divide $N$ by a large number of integers, for example all the primes less than $\sqrt{N}$, it was only necessary to compute some integer $S$ and test whether $N \mid S$.

Throughout his several papers on $U_n$ and $V_n$, Lucas alluded to the problem of extending or generalizing these functions and offered various suggestions by which this might be done. However, in spite of these ideas, he seems never to have produced any consistent theory that was analogous to his work on the Lucas functions.

On examining the material in [Luc76], [Luc78], [Luc80], [Luc91a] and [Luc91b], we note several properties of Lucas's investigation into his functions and those that he might have considered as proper generalizations. We certainly see that he was interested in functions satisfying linear recurring sequences; these functions should be symmetric functions of the zeros of a defining polynomial with rational (in practice, usually integral) coefficients, and there is more than one function to be considered. He seems to have been particularly interested in defining polynomials of degree three or four. He indicated the need to find addition and multiplication formulas involving these functions; this is certainly what he did in order to prove the many properties of his own functions. His method of approach was to use empirical techniques to attempt to elucidate what the laws of apparition and repetition for these functions would be, and from this material he should be able, as he did in the case of $U_n$ and $V_n$, to derive primality testing algorithms.

Laisant raised the intriguing possibility, through a question in *L'Intermédiaire des mathématiciens* [Lai96], that Lucas was considering three functions that were symmetric functions of $\alpha$, $\beta$ and $\gamma$, one of which was $S_n = \alpha^n + \beta^n + \gamma^n$; what were the other two functions? In his attempt to interpret Lucas's writings, Bell [Bel24] considered three functions, which he denoted as $x_n$, $y_n$, $z_n$. These can be most easily described by the equation

$$\alpha^n = x_n + y_n\alpha + z_n\alpha^2,$$

with similar expressions involving $\beta$ and $\gamma$. Clearly, these functions are symmetric functions of $\alpha$, $\beta$, $\gamma$. However, none of these functions is $S_n$; furthermore, these functions were known to Lucas (see pp. 305–306 of [Luc91b]), who mentioned them in a more general context without further comment. If these were the functions he was thinking about, it seems peculiar that he would not have mentioned something about them. Further properties of $x_n$, $y_n$ and $z_n$ were discussed by Ward [War31a] and Mendelsohn [Men62].

It is possible that Lucas had intended to publish his findings concerning the extension of his functions in one of the later volumes of *Théorie des nombres*. We know that he was considering the publication of additional books in this series (see the latter part of Chapter 6 of [Déc99]), and Harkin [Har57] has pointed out a short table of contents for Volume II: Divisibility and Algebraic Irreducibility, Binomial Congruences and Primitive roots. However, in response to a question raised by G. de Rocquigny concerning the possible appearance of the second and third volumes of *Théorie des nombres*, Delannoy, Laisant and Lemoine [DLL95] replied:

> *A careful examination of the papers left by Ed. Lucas has led us to this conclusion, that contrary to our first hopes, it would be very difficult to publish a continuation to the* Théorie des nombres, *of which only the first volume has appeared.*

In spite of the lack of information concerning it, the problem of extending or generalizing the Lucas functions has inspired a great deal of work. Some early attempts at this are mentioned in Chapter XVII of the first volume of [Dic19]. In the next section, we will briefly describe some of these and some of the more modern investigations into this problem.

## 3.2. Previous extensions of the Lucas functions

One of the earliest attempts to extend the Lucas functions was done in 1880 by de Longchamps [dL80]. If we put $R = \alpha\beta\gamma$, where $\alpha$, $\beta$ and $\gamma$ are the zeros of a cubic polynomial $f(x)$, de Longchamps considered $D_n$, $E_n$ and $A_n$ (this is, in fact, a modification of the original de Longchamps notation, as we have replaced his $S_n$ by $A_n$) where

$$\begin{cases} R^n D_n = (\alpha^n + \beta^n)(\beta^n + \gamma^n)(\gamma^n + \alpha^n), \\ R^n E_n = \dfrac{(\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)}{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)}, \\ A_n = \alpha^n + \beta^n + \gamma^n, \end{cases}$$

to be the degree three recurring function analogs of the Lucas functions. Are these the three functions to which Laisant was referring? They would certainly have been known to Lucas because he was the session chair for the talk in which de Longchamps presented his results. In fact, de Longchamps showed how to express $D_n$ and $E_n$ in terms of the coefficients of $f(x)$. However, Lucas would likely not have been comfortable with the fact that the first two of these functions are not necessarily integral. Also, in [Luc78], Lucas had certainly mentioned a more general version of the function $\Delta(\alpha^n, \beta^n, \gamma^n)/\Delta(\alpha, \beta, \gamma)$ that de Longchamps denoted by $R^n E_n$. This seems to be all that de Longchamps wrote concerning this topic because the list of his papers in [Laz07] does not contain any other paper devoted to this subject.

Lehmer [Leh30] extended the Lucas functions by replacing the parameter $P$ by $\sqrt{R}$, where $R$ is an integer coprime to $Q$; however, the resulting sequences are no longer integers for all $n$. Lehmer's functions were later generalized by Williams [Wil76], but in spite of the successes of the theory of Lehmer's extension and its generalization, there is no reason to believe that this was the direction in which Lucas was looking to extend his functions.

Carmichael [Car20], Ward [War31b, War31c, War33, War36, War37, War55] and Engstrom [Eng31] investigated the arithmetical theory of linear recurring sequences, but they did not produce a set of functions which were analogous to Lucas's functions $U_n$ and $V_n$. One of the most important properties of Lucas's function $U_n$ is that it satisfies the condition of being a divisibility sequence; that is, the sequence of integers $\{U_n\}$, with $n > 0$, is such that if $m \mid n$, then $U_m \mid U_n$. Lucas was very aware of this property of $U_n$ and made heavy use of it in developing his theory.

Williams [Wil69, Wil72a, Wil77] generalized the Lucas functions, but while his functions satisfy a linear recurrence, they are not symmetric functions of the zeros of a polynomial $f(x)$. Furthermore, they are not always integers unless the coefficients of $f(x)$ obey certain properties. Again, these functions do not seem to be those for which Lucas was searching.

Ballot [Bal99] developed a generalization which, for cubics $f(x)$ of discriminants of the form $M^3 \pm 1$, coincides with the generalization given in [Wil69]. This line of study first appeared in Chapter 4 of [Bal95], with

$$U_n^* = \delta^{-1}[(\gamma - \beta)\alpha^n + (\alpha - \gamma)\beta^n + (\beta - \alpha)\gamma^n],$$

and up to three associated integral companion sequences given by

$$V_n^i = \delta^{-1}[(\gamma - \beta)\epsilon_{1,i}\alpha^n + (\alpha - \gamma)\epsilon_{2,i}\beta^n + (\beta - \alpha)\epsilon_{3,i}\gamma^n], \quad \text{for } i = 1, 2, 3,$$

where $\epsilon_{j,i} = 1$ if $j \neq i$, and $\epsilon_{i,i} = -1$. Each prime $p$ divides $(U_n^*, U_{n+1}^*)$ for some $n \geq 0$. The least such $n > 0$ is the rank of $p$, and primes that divide $(V_n^i, V_{n+1}^i)$, for some $n$ and some $i = 1$, 2 or 3, are prime factors of the de Longchamps sequence $L_n = R^n D_n$. Note that depending on the reducibility of $f(x)$ some of the $V_n^i$'s may not be integral, but their product is.

### 3.3. Our objective

While many researchers have looked directly or peripherally at the problem of extending Lucas's functions, none of them seems to have produced the kind of results that Lucas was seeking. In what follows, we will offer a new suggestion as to how Lucas might have wanted to extend his functions. This is based on a very simple variant of de Longchamps's original suggestion.

We begin with a cubic polynomial $f(x) = x^3 - Px^2 + Qx - R$, where $P$, $Q$ and $R$ are integers and we put

$$\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha),$$

and

$$\Delta = \delta^2 = P^2Q^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2,$$

where $\alpha$, $\beta$ and $\gamma$ are the zeros of $f(x)$. We will assume that $\delta \neq 0$. We next define $C_n$ and $W_n$ by

$$\begin{aligned} \delta C_n &= (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n) \\ &= (\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}) - (\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n) \end{aligned}$$

and

$$W_n = (\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}) + (\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n).$$

Note that $C_n$ is the same as Lucas's $\dfrac{\Delta(\alpha^n, \beta^n, \gamma^n)}{\Delta(\alpha, \beta, \gamma)} (= R^nE_n)$ and $W_n = L_n - 2R^n$, where

$$L_n = R^nD_n = (\alpha^n + \beta^n)(\beta^n + \gamma^n)(\gamma^n + \alpha^n).$$

Both $C_n$ and $W_n$ are symmetric functions of $\alpha$, $\beta$ and $\gamma$ and are therefore integers for all non-negative values of $n$. It is these functions that we will use as our extensions of the Lucas functions $U_n$ and $V_n$. Observe that $\{C_n\}$ is a divisibility sequence.

In the previous section we listed the most important properties of the Lucas functions $U_n$ and $V_n$; most of these were known to Lucas, and can be found in his memoir [Luc78]. It would be reasonable to expect that he would want to extend these results. In the succeeding sections we will develop analogous results involving $C_n$ and $W_n$. These will include, among several other items, the addition formulas, the multiplication formulas, the laws of apparition and repetition and some primality testing results. What is most remarkable in this entire investigation is the need for only two functions, not three. In the next section we will define our generalization of $C_n$ and $W_n$ of the Lucas functions for an arbitrary degree $m$ polynomial, not just for the cubic case $m = 3$.

## 4. A new cubic generalization of the Lucas functions

### 4.1. De Longchamps's method

Denoting again $R^nD_n$ by $L_n$ and $R^nE_n$ by $C_n$, so as to match the notation of other generalizations, de Longchamps's work yielded a few interesting results, including the multiplicative formula

$$C_{2n} = L_nC_n.$$

He also developed the following identities

$$L_n = R^n(\sigma_n + \tau_n + 2) \quad \text{and} \quad \delta C_n = R^n(\sigma_n - \tau_n),$$

where

$$\sigma_n = \frac{\alpha^n}{\beta^n} + \frac{\beta^n}{\gamma^n} + \frac{\gamma^n}{\alpha^n} \quad \text{and} \quad \tau_n = \frac{\beta^n}{\alpha^n} + \frac{\alpha^n}{\gamma^n} + \frac{\gamma^n}{\beta^n}.$$

However, it should be stated that neither $\{\sigma_n\}$ nor $\{\tau_n\}$ are integer sequences.

If we let $S_n = \alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}$, and $T_n = \alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n$, then

$$\delta C_n = S_n - T_n \quad \text{and} \quad L_n = S_n + T_n + 2R^n.$$

Also,

$$\begin{aligned} S_nT_n &= R^nA_n^3 + B_n^3 - 6R^nA_nB_n + 9R^{2n} \\ &= R^nA_{3n} + B_{3n} + 3R^{2n}, \end{aligned}$$

where $B_n$ is defined in the next section.

### 4.2. Another cubic generalization

In an attempt to develop a theory analogous to that of Lucas's functions, the following method was proposed by Williams [Wil98]. Again, there are three sequences defined in this generalization. As in the last method, let $\alpha$, $\beta$ and $\gamma$ be the zeros of $X^3 - PX^2 + QX - R$, where $P$, $Q$ and $R$ are integers. Now define

$$\begin{cases} A_n = \alpha^n + \beta^n + \gamma^n, \\ B_n = \alpha^n\beta^n + \beta^n\gamma^n + \gamma^n\alpha^n, \\ C_n = \left(\dfrac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\dfrac{\beta^n - \gamma^n}{\beta - \gamma}\right)\left(\dfrac{\gamma^n - \alpha^n}{\gamma - \alpha}\right). \end{cases}$$

Rather than a second order linear recurrence as in identity (1) for the Lucas case, there is the following result for $A_n$ and $B_n$.

**Theorem 4.1.** *The sequences $A_n$ and $B_n$ respectively satisfy the third order recurrence formulas*

$$t_{n+3} = Pt_{n+2} - Qt_{n+1} + Rt_n \quad \textit{and} \quad t_{n+3} = Qt_{n+2} - RPt_{n+1} + R^2t_n.$$

If we write (10) as $\Delta U_n^2 = V_n^2 - 4Q^n$, then the following theorem is a useful generalization for this cubic case.

**Theorem 4.2.** *We have*

$$\Delta C_n^2 = A_n^2B_n^2 + 18A_nB_nR^n - 4B_n^3 - 4A_n^3R^n - 27R^{2n}$$

*and*

$$27\Delta C_n^2 = 4(A_n^2 - 3B_n)^3 - (27R^n + 2A_n^3 - 9A_nB_n)^2.$$

The following theorem provides some addition formulas for $A_n$ and $B_n$.

**Theorem 4.3.** *We have*

$$A_{n+m} = A_nA_m - (B_nA_{m-n} - R^nA_{m-2n})$$

*and*

$$B_{n+m} = B_nB_m - R^n(A_nB_{m-n} - R^nB_{m-2n}).$$

**Corollary 4.4.** *We have*

$$\sigma_{n+m} = \sigma_n\sigma_m - \tau_n\sigma_{m-n} + \sigma_{m-2n}$$

*and*

$$\tau_{n+m} = \tau_n\tau_m - \sigma_n\tau_{m-n} + \tau_{m-2n}.$$

Note that historically Corollary 4.4 was discovered by de Longchamps in his original paper [dL80].

### 4.3. Our generalization

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the roots of the degree $m$ polynomial

$$X^m - P_{m-1}X^{m-1} + P_{m-2}X^{m-2} - \cdots + (-1)^m P_0,$$

where $P_{m-1}, \ldots, P_0$ are integers. Further, if we let $\delta = \prod_{1\le i<j\le m}(\alpha_j - \alpha_i)$ then $\Delta = \delta^2$ is the discriminant of the above polynomial. It will be assumed that $\Delta \neq 0$. Lastly, let

$$V = \begin{bmatrix} 1 & \alpha_1^n & \alpha_1^{2n} & \ldots & \alpha_1^{(m-1)n} \\ 1 & \alpha_2^n & \alpha_2^{2n} & \ldots & \alpha_2^{(m-1)n} \\ 1 & \alpha_3^n & \alpha_3^{2n} & \ldots & \alpha_3^{(m-1)n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_m^n & \alpha_m^{2n} & \ldots & \alpha_m^{(m-1)n} \end{bmatrix}$$

be a Vandermonde matrix. Then we can define generalized Lucas sequences of degree $m$ as follows:

$$\delta C_n = \det V = \prod_{1\le i<j\le m} (\alpha_j^n - \alpha_i^n).$$

Or, using the Leibniz formula,

$$\delta C_n \ = \ \sum_{\sigma\in S_m} sgn(\sigma)\alpha_1^{n(\sigma(1)-1)} \cdots \alpha_m^{n(\sigma(m)-1)}$$

and we define $W_n$ by

$$W_n = \sum_{\sigma\in S_m} \alpha_1^{n(\sigma(1)-1)} \cdots \alpha_m^{n(\sigma(m)-1)},$$

where $S_m$ denotes the set of permutations of $\{1, 2, \ldots, m\}$, and $sgn(\sigma)$ denotes the sign of the permutation $\sigma$.

It can be readily verified for the case $m = 2$ that this generalization is, in fact, just the historic Lucas sequence, that is, $C_n = U_n$ and $W_n = V_n$. For the case $m = 3$, we fall back on the two sequences $C_n$ and $W_n$ presented in Subsection 3.3. In an effort to achieve simplicity and clarity with the new generalization, we will restrict ourselves to the case where $m = 3$. The theorem below is an extension of identity (1).

**Theorem 4.5.** *For a fixed $m$, the sequences $C_n$ and $W_n$ satisfy the recurrence formula*

$$X_{n+6m} = a_1X_{n+5m} - a_2X_{n+4m} + a_3X_{n+3m} - a_4X_{n+2m} + a_5X_{n+m} - a_6X_n,$$

*where*

$$\begin{cases} a_1 = W_m, & a_2 = (W_m^2 - \Delta C_m^2)/4 + R^m W_m, \\ a_3 = R^m(W_{2m} + 2R^m W_m + 2R^{2m}), & a_4 = R^{2m}a_2, \\ a_5 = R^{4m}a_1, & a_6 = R^{6m}. \end{cases}$$

**Proof.** For fixed $n$ and $m$, the sequences $(C_{n+mk})_{k\geq 0}$ and $(W_{n+mk})_{k\geq 0}$ are linear combinations of the $k$-th powers of $\alpha^m\beta^{2m}$, $\beta^m\gamma^{2m}$, $\gamma^m\alpha^{2m}$, $\alpha^{2m}\beta^m$, $\beta^{2m}\gamma^m$ and $\gamma^{2m}\alpha^m$, and these 6 quantities are the zeros of

$$x^6 - a_1x^5 + a_2x^4 - a_3x^3 + a_4x^2 - a_5x + a_6. \qquad \square$$

Since, as observed in Section 4.1,

$$\delta C_n = S_n - T_n \quad \text{and} \quad W_n = S_n + T_n,$$

we find the important formulas

$$S_n = R^n\sigma_n = \frac{W_n + \delta C_n}{2} \quad \text{and} \quad T_n = R^n\tau_n = \frac{W_n - \delta C_n}{2}\cdot$$

Also we have that

$$\begin{aligned} \frac{W_n^2 - \Delta C_n^2}{4} &= S_nT_n = 3R^{2n} + R^nA_{3n} + B_{3n} \\ &= R^nA_n^3 + B_n^3 - 6R^nA_nB_n + 9R^{2n}. \end{aligned} \tag{16}$$

**Theorem 4.6.** *We have*

(a) $R^{2n}C_{-n} = -C_n$,

(b) $R^{2n}W_{-n} = W_n$.

Note that in the above theorem $R^{2n}$ is the logical analogue to $Q^n$ in the identities

$$Q^nU_{-n} = -U_n \quad \text{and} \quad Q^nV_{-n} = V_n$$

for the quadratic case.

### 4.4. Addition formulas for $W_n$ and $C_n$

As in other generalizations of Lucas sequences, there exist addition formulas for $C_n$ and $W_n$. These formulas build on de Longchamps's work, and are analogues of (4) and (5).

**Theorem 4.7.** *We have*

(a) $2W_{2n+m} = W_nW_{n+m} + \Delta C_nC_{n+m} - R^n(W_nW_m - \Delta C_nC_m - 2R^{2m}W_{n-m})$,

(b) $2C_{2n+m} = C_{n+m}W_n + C_nW_{n+m} - R^n(C_mW_n - C_nW_m + 2R^{2m}C_{n-m})$.

**Proof.** First, it is clear that

$$(W_n+\delta C_n)(W_{n+m}+\delta C_{n+m}) = W_nW_{n+m}+\delta C_nW_{n+m}+\delta C_{n+m}W_n+\Delta C_nC_{n+m}.$$

Using the fact that $R^n\sigma_n = \frac{W_n+\delta C_n}{2}$ we have

$$(W_n + \delta C_n)(W_{n+m} + \delta C_{n+m}) = (2R^n\sigma_n)(2R^{n+m}\sigma_{n+m}) = 4R^{2n+m}\sigma_n\sigma_{n+m}.$$

Corollary 4.4 and the fact $\sigma_{-n} = \tau_n$ yield

$$\sigma_n\sigma_{n+m} = \sigma_{2n+m} + \tau_n\sigma_m - \tau_{n-m}.$$

Hence

$$(W_n+\delta C_n)(W_{n+m}+\delta C_{n+m}) = 4R^{2n+m}(\sigma_{2n+m}+\tau_n\sigma_m-\tau_{n-m})$$

$$= 4R^{2n+m}\left(\frac{W_{2n+m}+\delta C_{2n+m}}{2R^{2n+m}}+\frac{W_n-\delta C_n}{2R^n}\frac{W_m+\delta C_m}{2R^m}-\frac{W_{n-m}-\delta C_{n-m}}{2R^{n-m}}\right)$$

$$= 2W_{2n+m}+2\delta C_{2n+m}+R^n(W_nW_m-\delta C_nW_m+\delta C_mW_n-\Delta C_nC_m$$

$$-2R^{2m}W_{n-m}+2\delta R^{2m}C_{n-m}).$$

Thus we may conclude

$$W_nW_{n+m}+\delta C_nW_{n+m}+\delta C_{n+m}W_n+\Delta C_nC_{n+m}$$

$$= 2W_{2n+m}+2\delta C_{2n+m}+\delta R^n(-C_nW_m+C_mW_n+2R^{2m}C_{n-m})$$

$$+R^n(W_nW_m-\Delta C_nC_m-2R^{2m}W_{n-m}).$$

We next use the identity

$$R^n\tau_n=\frac{W_n-\delta C_n}{2}$$

and manipulate $(W_n-\delta C_n)(W_{n+m}-\delta C_{n+m})$ with the additive identity for $\tau_n$ in Corollary 4.4. By adding and subtracting the resulting formula from that given above, we get the identities stated in (a) and (b). □

There are the following special cases of the previous theorem.

**Corollary 4.8.** *We have*

(a) $2W_{2n}=\Delta C_n^2+W_n^2-4R^nW_n$,

(b) $C_{2n}=C_n(W_n+2R^n)=C_nL_n$,

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

(d) $4C_{3n}=C_n(\Delta C_n^2+3W_n^2)$.

The next corollary is only a slight modification of the previous theorem, but it does put the identities in a nicer form by removing the subtractions in the subscripts.

**Corollary 4.9.** *We have*

(a) $$2W_{n+3m}=\Delta C_mC_{n+2m}+W_mW_{n+2m}-R^mW_mW_{n+m}$$
$$+R^m\Delta C_mC_{n+m}+2R^{3m}W_n,$$

(b) $$2C_{n+3m}=W_mC_{n+2m}+C_mW_{n+2m}-R^mW_mC_{n+m}$$
$$+R^mC_mW_{n+m}-2R^{3m}C_n.$$

**Theorem 4.10.** *We have*

$$4R^{2n-1}PQ = W_n^2-\Delta C_n^2+2(W_{n+1}C_n-C_{n+1}W_n)-2R(W_{n+1}C_{n-1}$$
$$-W_{n-1}C_{n+1})+2R^2(W_nC_{n-1}-W_{n-1}C_n).$$

This formula is an extension of the Lucas identity (10)

$$V_n^2-\Delta U_n^2=4Q'^n,$$

where $V_n = V_n(P', Q')$ and $U_n = U_n(P', Q')$. This can be justified as follows. Since $V_{-n} = V_n/Q'^n$ and $U_{-n} = -U_n/Q'^n$, we see that $R^2$ corresponds to $Q'$. Using the identity

$$2Q'^m U_{n-m} = V_m U_n - U_m V_n$$

we can see that

$$\begin{cases} -2Q'^n = V_{n+1}U_n - U_{n+1}V_n & \text{when } m = n+1 \text{ and } n = n, \\ -2Q'^{n-1} = V_n U_{n-1} - U_n V_{n-1} & \text{when } m = n \text{ and } n = n-1, \\ -2Q'^{n-1}P' = V_{n+1}U_{n-1} - U_{n+1}V_{n-1} & \text{when } m = n+1 \text{ and } n = n-1. \end{cases}$$

Replacing $Q'$ by $R^2$ in the above returns

$$\begin{cases} V_{n+1}U_n - U_{n+1}V_n = -2R^{2n}, \\ V_n U_{n-1} - U_n V_{n-1} = -2R^{2n-2}, \\ V_{n+1}U_{n-1} - U_{n+1}V_{n-1} = -2R^{2n-2}P'. \end{cases}$$

Also note that $U_2 + RU_1 = P' + R$. Using the above and replacing $W_m$ by $V_m$ and $C_m$ by $U_m$ into the identity in Theorem 4.10 we see that

$$\begin{aligned} V_n^2 - \Delta U_n^2 &= 4R^{2n-1}(P' + R) - 2(-2R^{2n}) + 2R(-2R^{2n-2}P') \\ &\quad +2R^2(-2R^{2n-2}) \\ &= 4R^{2n}. \end{aligned}$$

It is not surprising that Theorem 4.10 involves 6 objects: $W_{n-1}$, $W_n$, $W_{n+1}$, $C_{n-1}$, $C_n$ and $C_{n+1}$, as one may recall that both $\{W_n\}$ and $\{C_n\}$ satisfy an order 6 recurrence.

In view of the importance that the quantity $W_n - 6R^n$ will assume in later sections, we also point out that from Theorem 4.2 it is easy to deduce that

$$(W_n - 6R^n)^2 + 3\Delta C_n^2 = 4(A_n^2 - 3B_n)(B_n^2 - 3R^n A_n).$$

## 4.5. Multiplication formulas for $W_n$ and $C_n$

A general multiplicative result is shown in the following theorem and this result is our analogue to (13) and (14). It is at this point where our generalization begins to outperform the others. This is because other generalizations are missing the necessary multiplication formulas needed in order to develop arithmetic results. Also, in the following theorem, we introduce $\tilde{P}_n$ and $\tilde{Q}_n$ for the first time, where

$$\tilde{P}_n = W_n \quad \text{and} \quad \tilde{Q}_n = \frac{W_n^2 - \Delta C_n^2}{4}.$$

This notation for $\tilde{P}_n$ and $\tilde{Q}_n$ will be used throughout the rest of the paper.

**Theorem 4.11.** *For any integers* $m \geq 0$, *we have*

(a) $$W_{mn} = \sum_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(\lambda_0+\lambda_3)} \tilde{Q}_n^{\lambda_2} V_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n),$$

(b) $$\frac{C_{mn}}{C_n} = \sum_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(\lambda_0+\lambda_3)} \tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n).$$

*Here the sum is extended over the values $\lambda_i \in \mathbb{Z}$ such that*

$$\lambda_0, \lambda_1, \lambda_2, \lambda_3 \geq 0, \quad \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = m \quad \text{and} \quad \lambda_1 + 2\lambda_2 + 3\lambda_3 = m,$$

*$U_k$ is the Lucas function $U_k(\tilde{P}_n, \tilde{Q}_n)$, $\tilde{P}_n = W_n$ and $\tilde{Q}_n = (W_n^2 - \Delta C_n^2)/4$.*

**Proof.** First let $\sigma_1 = \alpha/\beta + \beta/\gamma + \gamma/\alpha = \sum r_i$, where the sum is over the three quantities $r_1 = \alpha/\beta$, $r_2 = \beta/\gamma$, and $r_3 = \gamma/\alpha$. Thus $\sigma_1$ is the first elementary function of degree three involving these three terms. Also

$$\tau_1 = \frac{\beta}{\alpha} + \frac{\gamma}{\beta} + \frac{\alpha}{\gamma} = \sum_{i \neq j} r_i r_j.$$

Thus $\tau_1$ is the second elementary function of degree three. Finally note

$$\sum_{i \neq j \neq k} r_i r_j r_k = r_1 r_2 r_3 = 1.$$

Hence we can use Waring's theorem (see, for example, [Mac15]) to see that

$$\sigma_n = \left(\frac{\alpha}{\beta}\right)^n + \left(\frac{\beta}{\gamma}\right)^n + \left(\frac{\gamma}{\alpha}\right)^n = \sum_{\lambda_1, \lambda_2, \lambda_3} (-1)^{n+k} \frac{n(k-1)!}{\lambda_1! \lambda_2! \lambda_3!} \sigma_1^{\lambda_1} \tau_1^{\lambda_2},$$

where $\lambda_1, \lambda_2, \lambda_3 \geq 0$, $\lambda_1 + \lambda_2 + \lambda_3 = k$ and $\lambda_1 + 2\lambda_2 + 3\lambda_3 = n$.

Setting $\lambda_0 = n - k$, so $(-1)^{n+k} = (-1)^{n-k} = (-1)^{\lambda_0}$, we can write the previous identity as

$$\sigma_n = \sum_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} (-1)^{\lambda_0} \frac{n(n - \lambda_0 - 1)!}{\lambda_1! \lambda_2! \lambda_3!} \sigma_1^{\lambda_1} \tau_1^{\lambda_2},$$

where $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \geq 0$, $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = n$ and $\lambda_1 + 2\lambda_2 + 3\lambda_3 = n$.

Similarly, we can use Waring's theorem to derive

$$\sigma_{mn} = \sum_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} (-1)^{\lambda_0} \frac{m(m - \lambda_0 - 1)!}{\lambda_1! \lambda_2! \lambda_3!} \sigma_n^{\lambda_1} \tau_n^{\lambda_2}$$

and

$$\tau_{mn} = \sum_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} (-1)^{\lambda_0} \frac{m(m - \lambda_0 - 1)!}{\lambda_1! \lambda_2! \lambda_3!} \tau_n^{\lambda_1} \sigma_n^{\lambda_2},$$

where $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \geq 0$, $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = m$ and $\lambda_1 + 2\lambda_2 + 3\lambda_3 = m$. This is the sum as stated in the theorem. Now, since $S_{mn} = R^{mn} \sigma_{mn}$ and $T_{mn} = R^{mn} \tau_{mn}$, we obtain

$$W_{mn} = S_{mn} + T_{mn} = \sum_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} (-1)^{\lambda_0} \frac{m(m - \lambda_0 - 1)!}{\lambda_1! \lambda_2! \lambda_3!} R^{mn} (\sigma_n^{\lambda_1} \tau_n^{\lambda_2} + \sigma_n^{\lambda_2} \tau_n^{\lambda_1}).$$

Or considering the term following the coefficient we obtain

$$\begin{aligned} R^{mn}(\sigma_n^{\lambda_1} \tau_n^{\lambda_2} + \sigma_n^{\lambda_2} \tau_n^{\lambda_1}) &= R^{(m - \lambda_1 - \lambda_2)n} (R^{n\lambda_1} \sigma_n^{\lambda_1} R^{n\lambda_2} \tau_n^{\lambda_2} + R^{n\lambda_2} \sigma_n^{\lambda_2} R^{n\lambda_1} \tau_n^{\lambda_1}) \\ &= R^{(\lambda_0 + \lambda_3)n} (S_n^{\lambda_1} T_n^{\lambda_2} + S_n^{\lambda_2} T_n^{\lambda_1}). \end{aligned}$$

Now we will employ some well-known results for Lucas sequences; that is,

$$S_n^\lambda = \left(\frac{W_n + \delta C_n}{2}\right)^\lambda = \frac{V_\lambda + \tilde{\delta}_n U_\lambda}{2},$$

and

$$T_n^\lambda = \left(\frac{W_n - \delta C_n}{2}\right)^\lambda = \frac{V_\lambda - \tilde{\delta}_n U_\lambda}{2},$$

where $U = U(\tilde{P}_n, \tilde{Q}_n)$, $V = V(\tilde{P}_n, \tilde{Q}_n)$, $\tilde{\Delta}_n = \Delta C_n^2$, $\tilde{\delta}_n = \delta C_n$ and $\tilde{P}_n$, $\tilde{Q}_n$ are as stated in the theorem.

So

$$\begin{aligned} S_n^{\lambda_1} T_n^{\lambda_2} + S_n^{\lambda_2} T_n^{\lambda_1} &= \frac{V_{\lambda_1} + \tilde{\delta}_n U_{\lambda_1}}{2} \frac{V_{\lambda_2} - \tilde{\delta}_n U_{\lambda_2}}{2} + \frac{V_{\lambda_2} + \tilde{\delta}_n U_{\lambda_2}}{2} \frac{V_{\lambda_1} - \tilde{\delta}_n U_{\lambda_1}}{2} \\ &= \frac{V_{\lambda_1} V_{\lambda_2} - \tilde{\Delta}_n U_{\lambda_1} U_{\lambda_2}}{2}. \end{aligned}$$

To complete the proof of (a), use the following identity known for Lucas sequences:

$$2Q^m V_{n-m} = V_n V_m - \Delta U_n U_m,$$

replacing $n = \lambda_1$, $m = \lambda_2$ and $\Delta = \tilde{\Delta}_n$. Hence

$$S_n^{\lambda_1} T_n^{\lambda_2} + S_n^{\lambda_2} T_n^{\lambda_1} = \tilde{Q}_n^{\lambda_2} V_{\lambda_1 - \lambda_2}.$$

Part (b) is proven similarly by expanding $\delta C_n = S_n - T_n$ via Waring's theorem. □

It is the general multiplication formulas that allow us to proceed with this cubic generalization. With them we are able to develop arithmetic properties for $C_n$ and $W_n$ in Section 5. Once we have arithmetic properties some primality testing can be done.

# 5. Arithmetic properties of $\{C_n\}$ and $\{W_n\}$

## 5.1. Introductory arithmetic results

To continue our generalization we need to develop arithmetic results that are logical analogues of the arithmetic results seen in Section 2 for Lucas sequences.

**Lemma 5.1.** *If* $(Q, R) = 1$, *then* $(B_n, R) = 1$, *for* $n > 0$.

**Lemma 5.2.** *If* $(Q, R) = 1$ *and* $2^\alpha \mid\mid (W_n, C_n)$, *then* $\alpha \in \{0, 1\}$. *If* $2 \mid W_n$, *then* $\tilde{Q}_n$ *is odd.*

The following result is a clear analogue of (15).

**Theorem 5.3.** *If* $(Q, R) = 1$, *then for* $n > 0$,

$$(W_n, C_n, R) \mid 2.$$

**Proof.** Let $p$ be any prime such that $p \mid (W_n, C_n, R)$. Since $p \mid W_n$ and $p \mid C_n$, we must have $p \mid W_n^2 - \Delta C_n^2$. Observe that by equation (16), $p \mid 4B_{3n}$. Also,

$$B_{3n} = B_n^3 - 3R^n A_n B_n + 3R^{2n},$$

so $p \mid 4B_n^3$. Since $(Q, R) = 1$, we have $(B_n, R) = 1$ by Lemma 5.1 but this implies $p \nmid B_n$, so $p = 2$. Indeed, by Lemma 5.2, we must have $(W_n, C_n, R) \mid 2$. □

**Theorem 5.4.** *The sequence $\{C_n\}$ is a divisibility sequence.*

**Proof.** Note that if $n = ms$, then

$$C_n(P, Q, R) = C_m(P, Q, R) \cdot C_s(A_m, B_m, R^m). \qquad \square$$

**Definition 5.5.** Given $m \in \mathbb{Z}$, let $r$ be the least positive integer, if it exists, such that $m \mid C_r$. This value is called the *rank of apparition of $m$ for the sequence $\{C_n\}$* and will be denoted by $r(m)$.

In Theorem 2.2 for the classic Lucas case, we had that if $m \mid U_k$, then $r(m) \mid k$. However, this is not necessarily true for $\{C_n\}$. It may be that $m \mid C_k$, yet $r(m) \nmid k$.

**Definition 5.6.** Let $r_1$ be the least positive integer for which we have $p \mid C_{r_1}$. For $i = 1, 2, \ldots, k$ define $r_{i+1}$ to be the least positive integer, if it exists, such that $p \mid C_{r_{i+1}}$, $r_{i+1} > r_i$ and $r_j \nmid r_{i+1}$ for any $j \le i + 1$. We define $r_1, r_2, \ldots, r_k$ to be the ranks of apparition of $p$ for $\{C_n\}$.

It will become clear that the number of ranks of apparition is finite. For example, if we let $P = 1$, $Q = 2$, $R = 3$ and $p = 7$, then $\{C_n\}$ has two ranks of apparition for the prime 7. In fact, $C_3 \equiv 0 \pmod{p}$ and $C_7 \equiv 0 \pmod{p}$. Also, if we let $P = 3$, $Q = 9$, $R = 7$ and $p = 31$, then $\{C_n\}$ has three ranks of apparition. This follows from $C_6 \equiv 0 \pmod{p}$, $C_{10} \equiv 0 \pmod{p}$ and $C_{15} \equiv 0 \pmod{p}$.

Our sequence $\{C_n\}$ also fails to satisfy the generalization of Corollary 2.3 where if $d = (m, n)$, then

$$(U_m, U_n) = |U_d|.$$

It can be that

$$(C_m, C_n) \neq |C_d|,$$

and $d = (m, n)$. For example, if $P = 3$, $Q = 9$, $R = 7$, then $(C_6, C_{10}) = 2^2 \cdot 5 \cdot 31$ and $C_2 = 2^2 \cdot 5$.

We have seen that many of Lucas's results have analogues when we assume that $(Q, R) = 1$. This is similar to Lucas's condition that $(P, Q) = 1$, and we will assume for the remainder of this work that $(Q, R) = 1$.

### 5.2. The law of repetition for $\{C_n\}$

The proof of the law of repetition for $\{C_n\}$ relies on the following main results. Two proofs for the following theorem can be found in [Roe09], one using algebraic number theory and a second in Appendix A, employing techniques that Lucas himself could have used.

**Theorem 5.7.** *Let $p$ be a prime such that $p \nmid 6R\Delta$, $p \mid C_n$ and $p \mid W_n - 6R^n$. Then $p^3 \mid C_n$ and $p^2 \mid W_n - 6R^n$.*

Next we define

$$K_m(X) = \sum \frac{(-1)^{\lambda_0} m(m - \lambda_0 - 1)!(\lambda_1 - \lambda_2)}{\lambda_1!\lambda_2!\lambda_3!} X^{\lambda_1+\lambda_2-1},$$

where the sum is extended over the values $\lambda_i \in \mathbb{Z}$ such that

$$\lambda_0, \lambda_1, \lambda_2, \lambda_3 \geq 0, \quad \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = m \quad \text{and} \quad \lambda_1 + 2\lambda_2 + 3\lambda_3 = m.$$

**Theorem 5.8.** *If* $D(X) = X^2 - 2X - 3 = (X-3)(X+1)$, *then*

$$K_m(X) = \frac{m}{X-3}\left[\left(\frac{X-1+\sqrt{D(X)}}{2}\right)^m + \left(\frac{X-1-\sqrt{D(X)}}{2}\right)^m - 2\right].$$

**Theorem 5.9.** *Let* $X \in \mathbb{Z}$ *and* $p > 3$ *be a prime . If* $p \nmid X - 3$, *then*

$$K_p(X) \equiv p \pmod{p^2}.$$

*If* $p \mid X - 3$, *then*

$$K_p(X) \equiv p^3 \pmod{p^4}.$$

In the proof of Theorem 5.8 in [Roe09] we make use of partial derivatives; Lucas as well often did this. See for example, Section XVII of [Luc78]. Our law of repetition for $\{C_n\}$, which relies on the observation that

$$\frac{C_{mn}}{C_n} \equiv R^{n(m-1)} K_m(W_n/2R^n) \pmod{F_n},$$

where $F_n$ is defined in (18) below, is provided by the next theorem.

**Theorem 5.10.** *Let* $p^\lambda \mid\mid C_n$, *with* $\lambda \geq 1$.

(a) *If* $p \geq 3$ *and* $p \mid W_n - 6R^n$, *then*

$$p^{\lambda+3\mu} \mid C_{p^\mu n}, \quad \text{with} \quad p^{\lambda+3\mu} \mid\mid C_{p^\mu n} \quad \text{for} \quad p^\lambda > 3.$$

(b) *If* $p \geq 3$ *and* $p \nmid W_n - 6R^n$, *then*

$$p^{\lambda+\mu} \mid\mid C_{p^\mu n}.$$

(c) *If* $p = 2$ *and* $2 \mid R$, *then*

$$\begin{cases} 2^{\lambda+\mu} \mid\mid C_{2^\mu n} & \text{for } \lambda > 1, \\ 2^{\lambda+\mu} \mid C_{2^\mu n} & \text{for } \lambda = 1. \end{cases}$$

(d) *If* $p = 2$ *and* $2 \nmid R$, *then*

$$\begin{cases} 2^{\lambda+2\mu} \mid C_{2^\mu n} & \text{for } \lambda > 1, \\ 2^{2\mu} \mid C_{2^\mu n} & \text{for } \lambda = 1. \end{cases}$$

Some additional precisions may be obtained for $p = 2$ and $2 \nmid \Delta R$ when $\lambda \geq 4$, details of which can be found in [Roe09]. In the case of the law of repetition for the Lucas functions $U_n$, we know that $p^{\lambda+\mu} \mid\mid U_{nmp^\mu}$ if $p \nmid m$ and $p^\lambda \mid\mid U_n$. This result does not generalize to $C_n$. For example, if $p \nmid W_n - 6R^n$ and $p \nmid 2R$, it is possible that $p^\lambda \mid\mid C_n$ and $p^{\lambda+1} \mid C_{mn}$, where $p \nmid m$. We note that

$$\left(\frac{W_n}{2R^n} - 3\right)\frac{C_{mn}}{C_n} \equiv m\left(-2 + V_m(W_n/2R^n - 1, 1)\right) \pmod{p}.$$

By Theorem 2.7 we know that $V_m(W_n/2R^n - 1, 1) \equiv 2 \pmod{p}$ when $m = p - \epsilon$, where

$$\epsilon = \left(\frac{(W_n/2R^n - 1)^2 - 4}{p}\right) = \left(\frac{(W_n - 6R^n)(W_n + 2R^n)}{p}\right).$$

It follows that if $\epsilon$ is not equal to zero, as will be most frequently the case, then $p \mid (C_{mn}/C_n)$ and $p \nmid m$.

### 5.3. The law of apparition for $\{C_n\}$

If a prime $p$ divides $R$, it is easy to see that

$$C_n \equiv Q^{n-1} U_n(P, Q) \pmod{p},$$

in which case the theory reduces to that of the Lucas function $U_n(P, Q)$. We will therefore assume that $p \nmid R$ in what follows.

We point out that

$$27\Delta = 4(P^2 - 3Q)^3 - (27R + 2P^3 - 9QP)^2.$$

When $p \mid \Delta$ and $p \neq 2$, the splitting field of $f(x) = x^3 - Px^2 + Qx - R \in \mathbb{F}_p[x]$ is $\mathbb{F}_p$, and we have two possible cases.

On the one hand, suppose that $p \mid P^2 - 3Q$. Here $f(x) \equiv (x - a)^3 \pmod{p}$ where $a \equiv P/3 \pmod{p}$ (if $p = 3$, then $3 \mid P$). In this case we can put $\alpha = \beta = \gamma = a$ in $\mathbb{F}_p$. Now in $\mathbb{F}_p$,

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = \alpha^{n-1} + \beta\alpha^{n-2} + \beta^2\alpha^{n-3} + \cdots + \beta^{n-1} = na^{n-1},$$

so it follows that

$$C_n \equiv n^3 a^{3(n-1)} \pmod{p} \quad \text{and} \quad W_n \equiv 6a^{3n} \pmod{p}.$$

We may then conclude that $p \mid C_n$ if and only if $p \mid n$. Also, if $p \mid C_n$, then $p \mid W_n - 6R^n$.

On the other hand, suppose that $p \nmid P^2 - 3Q$. In this case $f(x) \equiv (x - a)^2(x - b) \pmod{p}$, where

$$a \equiv \frac{PQ - 9R}{2(P^2 - 3Q)} \pmod{p} \quad \text{and} \quad b \equiv \frac{P^3 - 4PQ + 9R}{P^2 - 3Q} \pmod{p}.$$

Hence we can put $\alpha = \beta = a \neq 0$ and $\gamma = b \neq 0$ in $\mathbb{F}_p$. Put $P' \equiv P - a \pmod{p}$ and $Q' \equiv a^2 - Pa + Q \pmod{p}$. One can see that since $a^2 b \equiv R \pmod{p}$, we get $ab \equiv R/a \equiv a^2 - Pa + Q \pmod{p}$. Also, $2a + b \equiv P \pmod{p}$, and therefore $a + b \equiv P - a \pmod{p}$. We use these results to obtain

$$\begin{aligned} C_n &= \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\frac{\beta^n - \gamma^n}{\beta - \gamma}\right)\left(\frac{\gamma^n - \alpha^n}{\gamma - \alpha}\right) \\ &= na^{n-1}\left(\frac{a^n - b^n}{a - b}\right)^2 \end{aligned}$$

in $\mathbb{F}_p$. Thus,

$$C_n \equiv na^{n-1} U_n^2(P', Q') \pmod{p}.$$

It is also true that $\left(\frac{\Delta'}{p}\right) = 1$, as

$$\Delta' = P'^2 - 4Q' \equiv (a-b)^2 \equiv \frac{(27R + 2P^3 - 9PQ)^2}{4(P^2 - 3Q)^2} \equiv P^2 - 3Q \pmod{p}.$$

Thus $p \,|\, C_n$ if and only if $p \,|\, n$ or $p \,|\, U_n(P', Q')$ since $p \nmid a$. If $p \,|\, a$ or $p \,|\, Q'$, then $p \,|\, R$, which is a contradiction. Since the rank of apparition of $p$ in $U_n(P', Q')$ is a divisor $r$ of $p-1$, we can say that $p \mid C_n$ if and only if either $p \mid n$ or $r \mid n$. Since $(r, p) = 1$ we have two ranks of apparition in this case. We also note that since

$$W_n - 6R^n \equiv 2a^n \Delta' U_n^2(P', Q') \pmod{p},$$

we see that $p \mid W_n - 6R^n$ if and only if $n$ is a multiple of $r$.

It can be shown that $r(2)$ always exists and is unique (Theorem 4.15 of [Roe09]). The case for $p = 3$ can be handled explicitly by calculation and is done in [Roe09]. By a computer search through all possible residue classes of $P$, $Q$, and $R$ modulo 3 it can be shown that there always exists at least one rank of apparition for 3 in $\{C_n\}$ as long as $(Q, R) = 1$. Also, $r(3) \leq 13 = 3^2 + 3 + 1$. Note also that if $3 \nmid \Delta$ and $3 \mid C_n$, then $r(3) \mid n$.

We now deal with those primes $p$ such that $p \nmid 6\Delta R$. The law of apparition for $\{C_n\}$ is more difficult than that for $\{U_n\}$. This is largely due to the fact that $\{C_n\}$ can have multiple ranks of apparition, as has been seen. Just how many ranks of apparition $\{C_n\}$ actually has, modulo a prime $p$, is dependent on the splitting behaviour of $f(x)$ modulo $p$. Following Adams and Shanks [AS82] we will characterize the primes that do not divide $6\Delta R$ as follows.

Let $f(x) = x^3 - Px^2 + Qx - R$ and $p \nmid 6R\Delta$. There are three possibilities for the splitting field $\mathbb{K}$ of $f(x) \in \mathbb{F}_p[x]$ :

(1) if $\mathbb{K} = \mathbb{F}_p$, we say that $p$ is an *$S$ prime*;

(2) if $\mathbb{K} = \mathbb{F}_{p^2}$, we say that $p$ is a *$Q$ prime*;

(3) if $\mathbb{K} = \mathbb{F}_{p^3}$, we say that $p$ is an *$I$ prime*.

Determining the type of a prime $p$ is important, since its type dictates where $C_n$ equals 0 in $\mathbb{K}$. This is also an old problem and several references to how it can be solved are mentioned in Chapter VIII of the first volume of [Dic19] (see also [WZ74] and [Mül04]). We summarize these results in the following theorem.

**Theorem 5.11.** *Suppose that $p$ is a prime and $p \nmid 6\Delta R$.*

(a) *If $\left(\frac{\Delta}{p}\right) = -1$, then $p$ is a $Q$ prime.*

(b) *If $\left(\frac{\Delta}{p}\right) = 1$, $p \equiv \epsilon \pmod{3}$, $A = 2P^3 - 9QR + 27R$, $B = P^3 - 3Q$ and $p \mid U_{\frac{p-\epsilon}{3}}(A, B^3)$, then $p$ is an $S$ prime; otherwise, $p$ is an $I$ prime.*

We will now develop the law of apparition for a prime $p$ in $\{C_n\}$. First we determine the number of ranks of apparition of a $Q$ prime.

**Theorem 5.12.** *Let $p$ be a $Q$ prime and $\alpha$, $\beta$, $\gamma$ be the zeros of $f(x)$ in $\mathbb{F}_{p^2}$, where $\beta \notin \mathbb{F}_p$. Then $p \mid C_m$ if and only if $\beta^m = \beta^{pm}$.*

**Corollary 5.13.** *If $p$ is a $Q$ prime, then $p \mid C_{p+1}$.*

**Corollary 5.14.** *Let $p$ be a $Q$ prime. Then $p$ can only have one rank of apparition, $r$, in $\{C_n\}$ and $r \mid p+1$.*

**Corollary 5.15.** *If $p$ is a $Q$ prime, $r$ is its rank of apparition in $\{C_n\}$ and $p \mid C_n$, then $r \mid n$.*

Note that if $p$ is a $Q$ prime, then

$$W_{p+1} \equiv 2\alpha^4\beta\gamma + 2\beta^3\gamma^3 + 2R^3 \pmod{p}.$$

This will not be useful to us here; however, we can see that

$$W_{p^2-1} \equiv 6 \pmod{p}.$$

**Theorem 5.16.** *If $p$ is an $I$ prime, then $p \mid C_{p^2+p+1}$.*

For an $I$ prime $p$,

$$W_{p^2+p+1} \equiv 6R^3 \pmod{p}.$$

**Corollary 5.17.** *Let $p$ be an $I$ prime. Then $p$ can only have one rank of apparition $r$ in $\{C_n\}$ and $r \mid p^2+p+1$.*

**Corollary 5.18.** *Let $p$ be an $I$ prime. If $r$ is the rank of apparition of $p$ in $\{C_n\}$ and $p \mid C_n$, then $r \mid n$.*

Thus, the situation with $Q$ and $I$ primes parallels that of primes that divide $U_n$. That is, we know that if a prime $p$ divides $U_n$, then the rank of apparition $\omega = \omega(p)$ of $p$ in $\{U_n\}$ must divide $n$. However, the situation with $S$ primes can be different.

**Theorem 5.19.** *Let $p \nmid 6\Delta R$ and $p$ be an $S$ prime. Then $p \mid C_{p-1}$.*

Once more we note that under these circumstances

$$W_{p-1} \equiv 6 \pmod{p}.$$

**Corollary 5.20.** *If $p$ is an $S$ prime and $p \nmid 6\Delta R$, then $p$ may have at most 3 ranks of apparition in $\{C_n\}$ and each rank of apparition divides $p-1$.*

**Corollary 5.21.** *If $p$ is an $S$ prime and $p \mid C_n$, then at least one of the ranks of apparition of $p$ in $\{C_n\}$ must divide $n$.*

We have in fact shown that there exists an infinite set of primes $\mathcal{P}$ such that for each $p$ in $\mathcal{P}$ there is a cubic recursion in which $p$ has three distinct ranks (see [Roe09], Theorem 4.27).

## 6. Arithmetic properties of $\{D_n\}$ and $\{E_n\}$

### 6.1. Definition of the divisibility sequence $\{D_n\}$

While, as we have seen, $C_n$ is analogous to the Lucas function $U_n$ in many respects, there are a number of significant differences between the arithmetic behaviour of $C_n$ and $U_n$. This is particularly the case in the law of repetition and the law of apparition, where it is possible to have more than one rank of apparition for $\{C_n\}$. In the law of repetition for a prime $p$ such that $p \mid C_n$, it is important to know whether or not $p$

divides the quantity $W_n - 6R^n$. We often have the case of a prime $p$ dividing both $C_n$ and $W_n - 6R^n$. In view of this, we define

$$D_n = gcd(C_n, W_n - 6R^n).$$

This is not as peculiar as it might seem at first. For if we look at the formula for $W_n - 6R^n$ in terms of $\alpha$, $\beta$ and $\gamma$, we see that the corresponding formula involving $\alpha$ and $\beta$ of the Lucas functions would be

$$\alpha^{2n} + \beta^{2n} - 2\alpha^n\beta^n = V_{2n} - 2Q^n.$$

This is because if we consider $W_n - 6R^n$ to be a polynomial in $\alpha^n$, $\beta^n$ and $\gamma^n$, then it is of degree three and the $\alpha^n\beta^n\gamma^n$ term is subtracted as many times as there are terms in the expression for $W_n$. Hence, the degree two counter part to this would be $\alpha^{2n} + \beta^{2n} - 2\alpha^n\beta^n$. However,

$$V_{2n} - 2Q^n = V_n^2 - 4Q^n = \Delta U_n^2 \text{ and } gcd(V_{2n} - 2Q^n, U_n) = U_n.$$

Notice that by Theorem 5.3 we have

$$gcd(D_n, R) \mid 2. \tag{17}$$

As we shall see below, it turns out that $D_n$ has arithmetic properties which are much more analogous to those of $U_n$ than does $C_n$.

**Theorem 6.1.** *The sequence $\{D_n\}$ is a divisibility sequence.*

**Proof.** In order to show that $\{D_n\}$ is a divisibility sequence we will first develop some results for the function $L_m(X)$. We define

$$L_m(X) = \sum \frac{(-1)^{\lambda_0} m(m - \lambda_0 - 1)!}{\lambda_1!\lambda_2!\lambda_3!} X^{\lambda_1+\lambda_2},$$

where the sum is extended over the values $\lambda_i \in \mathbb{Z}$ such that

$$\lambda_0, \lambda_1, \lambda_2, \lambda_3 \geq 0, \quad \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = m \quad \text{and} \quad \lambda_1 + 2\lambda_2 + 3\lambda_3 = m.$$

By Waring's theorem,

$$L_m(X) = \alpha_1^m + \alpha_2^m + \alpha_3^m,$$

where $\alpha_1$, $\alpha_2$ and $\alpha_3$ are the zeros of $Z^3 - XZ^2 + XZ - 1$ such that

$$\alpha_1 = 1, \quad \alpha_2 = \frac{X - 1 + \sqrt{D(X)}}{2}, \quad \alpha_3 = \frac{X - 1 - \sqrt{D(X)}}{2},$$

and $D(X) = (X - 3)(X + 1)$. We can then write

$$L_m(X) = 1 + \alpha_2^m + \alpha_3^m = 1 + V_m(X - 1, 1).$$

So, if $2 \nmid m$, it can be shown that

$$V_m(X - 1, 1) = V_1 \sum_{j=0}^{(m-1)/2} \binom{(m-1)/2 + j}{(m-1)/2 - j} D(X)^j.$$

To the contrary, if $2 \mid m$, then we can show that

$$V_m(X - 1, 1) = \sum_{j=0}^{m/2} \frac{m}{m/2 - j} \binom{m/2 + j - 1}{m/2 - j - 1} D(X)^j.$$

Now, by using results similar to those in Section 4.4 of [Roe09] and noting $\tilde{P}_n = W_n$, we have

$$W_{mn} \equiv 2 \sum_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} \left(\frac{\tilde{P}_n}{2}\right)^{\lambda_1+\lambda_2} R^{n(m-\lambda_1-\lambda_2)} \pmod{F_n}$$

where

$$F_n = \begin{cases} \Delta C_n^2 & \text{if } 2 \nmid C_n, \\ \Delta C_n^2/4 & \text{if } 2 \mid C_n. \end{cases} \tag{18}$$

Let $2^\gamma \mid\mid D_n$. Then $D_n/2^\gamma \mid F_n$, $2 \nmid D_n/2^\gamma$ and $(D_n/2^\gamma, R) = 1$. Moreover, let $G_n = D_n/2^\gamma$. Then

$$\begin{aligned} W_{mn} &\equiv 2R^{mn} \sum_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} \left(\frac{W_n}{2R^n}\right)^{\lambda_1+\lambda_2} \pmod{F_n} \\ &\equiv 2R^{mn} L_m(W_n/2R^n) \pmod{F_n}. \end{aligned}$$

If $m$ is odd,

$$L_m\left(\frac{W_n}{2R^n}\right) = 1 + \left(\frac{W_n}{2R^n-1}\right) \sum_{j=0}^{(m-1)/2} \binom{(m-1)/2+j}{(m-1)/2-j} \left(\frac{W_n}{2R^n+1}\right)^j \left(\frac{W_n}{2R^n-3}\right)^j.$$

Since $W_n/2R^n - 3 \equiv 0 \pmod{G_n}$,

$$L_m(W_n/2R^n) \equiv 1 + W_n/2R^n - 1 \equiv 3 \pmod{G_n}.$$

If $m$ is even,

$$\begin{aligned} L_m(W_n/2R^n) &= 1 + \sum_{j=0}^{m/2} \frac{m}{m/2-j} \binom{m/2+j-1}{m/2-j-1} \left(\frac{W_n}{2R^n+1}\right)^j \left(\frac{W_n}{2R^n-3}\right)^j \\ &\equiv 3 \pmod{G_n}. \end{aligned}$$

Thus, $W_{mn} \equiv 6R^{mn} \pmod{G_n}$, so $G_n \mid W_{mn} - 6R^{mn}$. It follows that if $\gamma = 0$, then $D_n \mid D_{nm}$.

If $\gamma = 1$, then since $2 \mid gcd(W_n, C_n)$, we have $2 \mid C_{mn}$, and since $\tilde{Q}_{mn}$ is an integer, we have $2 \mid W_{mn}$; thus, $D_n \mid D_{mn}$. If $\gamma > 1$, then $4 \mid C_n$ and $4 \mid W_n - 6R^n$. Recall that if $2^\alpha \mid\mid gcd(W_n, C_n)$, then $\alpha = 0$ or $\alpha = 1$ by Lemma 5.2. In this case $\alpha = 1$ and $2 \mid\mid W_n$. It follows from $4 \mid W_n - 6R^n$ that $R$ must be odd. Thus, since $2\gamma \geq \gamma + 2$, we have $2^\gamma \mid F_n$ and

$$\begin{aligned} W_{mn} &\equiv 2R^{mn} \sum_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} \left(\frac{W_n}{2R^n}\right)^{\lambda_1+\lambda_2} \pmod{2^\gamma} \\ &\equiv 6R^{mn} \pmod{2^\gamma}, \end{aligned}$$

so that $2^\gamma \mid W_{mn} - 6R^{mn}$. Consequently $D_n \mid W_{mn} - 6R^{mn}$, and further $D_n \mid D_{mn}$. Thus, if $n \mid m$, we get $D_n \mid D_m$. Therefore, like $\{U_n\}$ and $\{C_n\}$, $\{D_n\}$ is a divisibility sequence. □

## 6.2. The law of repetition for $\{D_n\}$

**Theorem 6.2.** *If $p$ is a prime, $p^\lambda \mid\mid D_n$ $(\lambda \geq 1)$ and $p \nmid m$, then $p^\lambda \mid\mid D_{mn}$.*

Our "law of repetition" for $\{D_n\}$ is provided in the following theorem.

**Theorem 6.3.** *If $p^\lambda \mid\mid D_n$ (with $p \neq 2$ and $p^\lambda \neq 3$), then*

$$\begin{cases} p^{\lambda+2} \mid\mid D_{pn} & \text{when } p^\lambda \mid\mid W_n - 6R^n, \\ p^{\lambda+3} \mid\mid D_{pn} & \text{otherwise}. \end{cases}$$

*Also, $p^{\lambda+2} \mid D_{pn}$ when $p^\lambda = 3$, and $p^{\lambda+1} \mid D_{pn}$ when $p = 2$. Furthermore, $p^{\lambda+1} \nmid D_{mn}$ if $p \nmid m$.*

Notice that if $p \notin \{2,3\}$, $p^\lambda \mid\mid W_n - 6R^n$ and $p^\lambda \mid\mid D_n$, then $p^{\lambda+2} \mid\mid W_{pn} - 6R^{pn}$ and therefore

$$p^{\lambda+2\mu} \mid\mid D_{p^\mu n}.$$

However, if $p^\lambda \mid\mid D_n$ and $p^{\lambda+1} \mid W_n - 6R^n$, it is not necessarily the case that

$$p^{\lambda+4} \mid\mid W_{pn} - 6R^{pn}.$$

The best we are able to show is that $p^{\lambda+3} \mid W_{pn} - 6R^{pn}$. If $p^{\lambda+3} \mid\mid W_{pn} - 6R^{pn}$, then we return to the previous condition and by induction we get

$$(p^{\lambda+1+2\mu} =)p^{\lambda+3+2(\mu-1)} \mid\mid D_{p^\mu n}.$$

Of course, this latter situation would never occur if the case of

$$p^\lambda \mid\mid D_n \quad \text{and} \quad p^{\lambda+1} \mid W_n - 6R^n$$

could not happen. This might be an infrequent occurrence, but unfortunately it does happen. For example, if $P = 257$, $Q = 2004$ and $R = 5389$, then $7^3 \mid\mid C_6$ and $7^4 \mid W_6 - 6R^6$.

Thus, we cannot provide an as complete law of repetition for $\{D_n\}$ as we were able to do for $\{C_n\}$. However, if $p^\lambda \mid\mid C_n$, $p^{\lambda+\kappa} \mid\mid W_n - 6R^n$ and $\kappa < \lambda - 2$, it can be shown that

$$p^{\lambda+3\mu} \mid\mid C_{p^\mu n} \quad \text{and} \quad p^{\lambda+\kappa+2\mu} \mid\mid W_{p^\mu n} - 6R^{p^\mu n}.$$

Hence, we get

$$p^{\lambda+3\mu} \mid\mid D_{p^\mu n}, \quad \text{for} \quad \mu \leq \kappa.$$

Note that if $\mu = \kappa$, then $\lambda + \kappa + 2\mu = \lambda + 3\mu$ and we return to the previous case. It follows that

$$p^{\lambda+\kappa+2\mu} \mid\mid D_{p^\mu n}$$

when $\mu > \kappa$. Unfortunately, if $\kappa \geq \lambda - 2$, it seems to be difficult to formulate a comprehensive law of repetition.

## 6.3. The law of apparition for $\{D_n\}$

**Definition 6.4.** Let $p$ be a prime and $\omega(p)$ be the least positive integer $n$, if it exists, such that $p \mid D_n$. We call this the *rank of apparition* of $p$ in $\{D_n\}$.

The next theorems build toward a result very comparable to Theorem 2.2. What is remarkable is that this is a result that did not hold for $\{C_n\}$. Hence, with the help of $\{D_n\}$ we are able to establish a more convincing analogue. We are now able to present an important result concerning $\omega(p)$.

**Theorem 6.5.** *If $p \nmid R$, then $\omega(p)$ must exist. Further, if $p \mid D_n$, then $\omega(p) \mid n$.*

**Corollary 6.6.** *If $p$ is a prime and $\omega(p)$ exists, then $\omega(p) \leq p^2 + p + 1$.*

Suppose $p \nmid R$ and $p^\alpha \mid D_n$. Let $\omega = \omega(p)$ and let $\omega(p^\alpha)$ denote the least positive integer $k$ such that $p^\alpha \mid D_k$. If $p^\alpha \mid D_\omega$, put $\nu = 0$; otherwise define $\nu \in \mathbb{Z}_{\geq 0}$ by

$$p^\alpha \mid D_{p^\nu \omega(p)} \quad \text{and} \quad p^\alpha \nmid D_{p^{\nu-1}\omega(p)}.$$

By our previous results concerning the law of repetition for $\{D_n\}$ such a $\nu$ must exist.

**Theorem 6.7.** *If $p \nmid R$ and $p^\alpha \mid D_n$, then $\omega(p^\alpha) = p^\nu \omega(p)$ and $\omega(p^\alpha) \mid n$.*

**Proof.** Since $p \mid D_n$, we must have $n = m\omega(p)$ for some $m \in \mathbb{N}$. Suppose that $p^\gamma \mid\mid m$ and put $m = m'p^\gamma$, where $p \nmid m'$. Since $p^\alpha \nmid D_{p^{\nu-1}\omega(p)}$, we must have $p^\alpha \nmid D_{m'p^{\nu-1}\omega(p)}$, so $\gamma > \nu - 1$. But $p^\alpha \mid D_{m'p^\nu\omega(p)}$, so $\gamma = \nu$. Furthermore, since $p^\alpha \mid D_{p^\nu\omega(p)}$, we must have $\omega(p^\alpha) = p^\nu\omega(p)$ and $\omega(p^\alpha) \mid n$. □

**Theorem 6.8.** *Suppose that $m \mid D_n$. Denote by $\omega(m)$ the least positive integer such that $m \mid D_{\omega(m)}$. Let*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

*Then $\omega(m) = lcm[\omega(p_i^{\alpha_i}); i = 1, 2, \ldots, k]$.*

**Proof.** Clearly $\omega(p_i^{\alpha_i}) \mid \omega(m)$ for $i = 1, 2, \ldots, k$. Since $D_n$ is a divisibility sequence the result follows. □

We may now prove the following theorem, which very much resembles Corollary 2.3. Again, this is another result that did not hold for $\{C_n\}$.

**Theorem 6.9.** *We have*

$$gcd(D_n, D_m) = D_{gcd(m,n)}.$$

**Proof.** Since $D_n$ is a divisibility sequence, we have $D_{gcd(m,n)} \mid D_n$, which implies

$$D_{gcd(m,n)} \mid gcd(D_n, D_m).$$

Let $p^\alpha \mid\mid gcd(D_n, D_m)$. Then $\omega(p^\alpha)$ exists, so $\omega(p^\alpha) \mid n$ and $\omega(p^\alpha) \mid m$. Hence $\omega(p^\alpha) \mid gcd(m, n)$, so $p^\alpha \mid D_{gcd(m,n)}$. Thus $gcd(D_n, D_m) = D_{gcd(m,n)}$. □

In Chapter 4 of [Roe09], we were able to develop a result somewhat akin to Carmichael's result in Theorem 2.4. Surprisingly, if we look at $\{D_n\}$ rather than $\{C_n\}$, we can in fact do much better. We have that

$$\frac{C_{mn}}{C_n} \equiv m^3 R^{n(m-1)} \pmod{gcd(F_n, W_n - 6R^n)},$$

where $F_n$ is as in (18). If $2^\nu \mid\mid C_n$ and $\nu > 1$, then $C_n \mid F_n$ and

$$\frac{C_{mn}}{C_n} \equiv m^3 R^{n(m-1)} \pmod{D_n}. \tag{19}$$

If $2 \mid\mid C_n$, then $\frac{C_{mn}}{C_n} \equiv m \pmod 2$ (see Theorem 4.10 of [Roe09]) and $C_n/2 \mid F_n$, so

$$\frac{C_{mn}}{C_n} \equiv m^3 R^{n(m-1)} \pmod{gcd\,(C_n/2, W_n - 6R^n)}.$$

Now $gcd(D_n, R) \mid 2$. If $gcd(D_n, R) = 1$, then $gcd\left(\frac{C_{mn}}{C_n}, D_n\right) \mid m^3$.

If $(D_n, R) = 2$, then $2 \mid\mid D_n$ by Lemma 5.2. Then $gcd\left(\frac{C_{mn}}{C_n}, D_n/2\right) \mid m^3$. Since $gcd(D_n/2, R) = 1$ and $gcd\left(\frac{C_{mn}}{C_n}, 2\right) \mid m$, we have $gcd\left(\frac{C_{mn}}{C_n}, D_n\right) \mid m^3$.

We next examine $gcd\left(\frac{D_{mn}}{D_n}, D_n\right)$. Let $p^\alpha \mid\mid gcd\left(\frac{D_{mn}}{D_n}, D_n\right)$. We will show that $p^\alpha \mid m^3$ when $p$ is a prime and $\alpha \geq 1$. This means of course that

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

We first observe that if $p \nmid m$, then $p \nmid D_{mn}/D_n$, which is a contradiction to Theorem 6.2, so $p \mid m$. If $\alpha < 4$, then $p^\alpha \mid m^3$. If $\alpha \geq 4$, then by the law of repetition for $D_n$, we know that $p^\lambda \mid\mid D_{mn}$, with $\lambda \leq 3\mu + \nu$, where $p^\nu \mid\mid D_n$ $(\nu \geq 4)$ and $p^\mu \mid m$. Thus if $p^\gamma \mid\mid D_{mn}/D_n$, then $\gamma = \lambda - \nu \leq 3\mu$, so $p^\gamma \mid m^3$. We now have the desired analogue of Theorem 2.4.

**Theorem 6.10.** *If $m \geq 1$ and $n \geq 1$, then*

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

**Theorem 6.11.** *Let $p$ be any prime such that $p \nmid 6\Delta R$. Put $T = p^2 - 1$ if $p$ is an $S$ or a $Q$ prime and $T = p^2 + p + 1$ otherwise. Then $p \mid D_T$.*

### 6.4. Preliminary results for $\{E_n\}$

While working on the sequences $\{W_n\}$ and $\{C_n\}$, several results were obtained concerning the sequence $\{E_n\}$, where $E_n = gcd(W_n, C_n)$. This sequence has a number of properties analogous to those of the Lucas sequence $\{V_n\}$. In the next several sections we will develop these properties. We begin with a result analogous to $gcd(U_n, V_n) \mid 2$ for Lucas functions.

**Theorem 6.12.** *If $gcd(Q, R) = 1$, then $gcd(D_n, E_n) \mid 6$.*

**Proof.** Suppose that $p$ is any prime such that $p \mid D_n$ and $p \mid E_n$. Since $p \mid W_n - 6R^n$, we must have $p \mid 6R^n$. Since $gcd(D_n, R) = gcd(E_n, R)$ and $gcd(D_n, R) \mid 2$ by (17), we can only have $p = 2$ or $p = 3$. If $3^2 \mid gcd(D_n, E_n)$, then $3 \mid R$, which is impossible. If $2^2 \mid gcd(D_n, E_n)$, then $2^2 \mid E_n$, which is also impossible by Lemma 5.2. Hence $gcd(D_n, E_n) \mid 6$. □

It is readily apparent that equation (11) implies $V_n \mid U_{2n}$. Similarly we have the following theorem.

**Theorem 6.13.** *We have $E_n \mid D_{3n}$.*

**Proof.** We can rework the identity

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

to see that

$$W_{3n} - 6R^{3n} \quad = \quad (W_n - 6R^n)\left(\frac{W_n^2 - \Delta C_n^2}{4}\right) + \Delta W_n C_n^2. \tag{20}$$

Recall again from Lemma 5.2 that if $gcd(Q, R) = 1$, then $2^\alpha \mid\mid gcd(W_n, C_n)$, so $\alpha = 0$ or $\alpha = 1$, and if $\alpha = 1$, then $\tilde{Q}_n = \frac{W_n^2 - \Delta C_n^2}{4}$ is odd.

We are now ready to show that $E_n \mid D_{3n}$. We know that $C_n \mid C_{3n}$. If $2 \nmid E_n$, then $E_n \mid \tilde{Q}_n$, so $E_n \mid W_{3n} - 6R^{3n}$ by equation (20). If $2 \mid E_n$, then $E_n/2$ is odd and $E_n/2 \mid \tilde{Q}_n$. Since $2 \mid W_n$, we have $2 \mid W_n - 6R^n$, so $E_n \mid (W_n - 6R^n)\tilde{Q}_n$ and $E_n \mid W_{3n} - 6R^{3n}$ by equation (20). Since $E_n \mid C_n$ and $C_n \mid C_{3n}$, we get $E_n \mid C_{3n}$ and $E_n \mid W_{3n} - 6R^{3n}$, so $E_n \mid D_{3n}$. □

We next derive some useful results concerning the primes which can divide $E_n$.

**Theorem 6.14.** *If* $gcd(Q, R) = 1$ *and* $p > 3$ *is a prime divisor of* $E_n$*, then* $p \equiv 1 \pmod 3$.

Thus, if $p$ is a prime such that $p > 3$, $p \equiv -1 \pmod 3$ and $p \mid D_{3n}$, we know that $p \nmid E_n$. Theorem 6.14 can now be generalized.

**Theorem 6.15.** *If* $p > 3$ *is a prime such that* $p \mid E_n$*, then* $p \equiv 1 \pmod{3^{\nu+1}}$*, where* $3^\nu \mid\mid n$.

**Proof.** Since $gcd(E_n, R) \mid 2$, we must have $p \nmid R$. Suppose that $p \mid E_n$. Then we know that $p$ cannot be an $I$ prime by Theorem 6.6 of [Roe09] and $p \equiv 1 \pmod 3$ by Theorem 6.14. We also have $p \mid D_{3n}$. If $p \mid D_n$, then $p \mid W_n$ and $p \mid W_n - 6R^n$, so $p \mid 6R^n$, which is a contradiction. Hence $p \nmid D_n$. Let $\omega$ be the rank of apparition of $p$ in $\{D_n\}$. We have $\omega(p) \mid 3n$ and $\omega(p) \nmid n$, as $p \mid D_{3n}$ and $p \nmid D_n$. So, if $3^\nu \mid\mid n$, then $3^{\nu+1} \mid \omega(p)$. Also, since $p$ is not an $I$ prime and $p \nmid 6R$, we have $\omega(p) \mid p$ or $\omega(p) \mid p^2 - 1$, by results seen in Theorem 6.5 for the $S$ and $Q$ prime cases. Hence,

$$\omega(p) \mid (p-1)(p+1),$$

so,

$$3^{\nu+1} \mid (p-1)(p+1).$$

Since $3 \mid \omega(p)$, we know $\omega(p) \nmid p$. Also, since $3 \mid p - 1$, we must have $3^{\nu+1} \mid p - 1$, so $p \equiv 1 \pmod{3^{\nu+1}}$. □

Lucas showed (Theorem 2.14) that if $p$ is an odd prime such that $p \mid V_n$, then $p \equiv \pm 1 \pmod{2^{\nu+1}}$, where $2^\nu \mid\mid n$. We next produce an analogue of this result. Recall that $V_n = U_{2n}/U_n$. We will consider those primes $p \notin \{2, 3\}$ such that $p \mid (D_{3n}/D_n)$.

**Theorem 6.16.** *If* $p > 3$ *is a prime such that* $p \mid (D_{3n}/D_n)$*, then* $p \equiv \pm 1 \pmod{3^{\nu+1}}$*, where* $3^\nu \mid\mid n$.

**Proof.** Since $p \mid D_{3n}$, we see that if $p \mid R$, then $p = 2$ by (17), which is not possible. Thus, $p \nmid R$. Also, since $gcd(D_{3n}/D_n, D_n) \mid 27$ by Theorem 6.10, we cannot have $p \mid D_n$. It follows by the same reasoning used in the proof of Theorem 6.15, that

$$3^{\nu+1} \mid (p-1)(p+1).$$

Hence $p \equiv \pm 1 \pmod{3^{\nu+1}}$. □

## 6.5. A law of repetition for $\{E_n\}$

**Theorem 6.17.** *If $p > 3$ is a prime such that $p^\mu \mid\mid E_n$, then $p^{\mu+1} \mid\mid E_{pn}$ for $\mu \geq 1$.*

**Proof.** We note that

$$p \,\left|\, \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!}\right.$$

unless $\lambda_1 = p$, $\lambda_0 = \lambda_2 = \lambda_3 = 0$. If $\lambda_1 = p$, then

$$\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) = U_p(\tilde{P}_n, \tilde{Q}_n) \quad \text{and} \quad \tilde{Q}_n^{\lambda_2} V_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) = V_p(\tilde{P}_n, \tilde{Q}_n).$$

Also, by Theorem 6.10 of [Roe09], $(p^\mu)^p \mid V_p(\tilde{P}_n, \tilde{Q}_n)$ and $(p^\mu)^{p-1} \mid U_p(\tilde{P}_n, \tilde{Q}_n)$. Now, since $p > 3$, we know that $2\mu + 1 < \mu(p-1)$ and thus

$$U_p(\tilde{P}_n, \tilde{Q}_n) \equiv V_p(\tilde{P}_n, \tilde{Q}_n) \equiv 0 \pmod{p^{2\mu-1}}.$$

Furthermore, $p^{2\mu} \mid \tilde{Q}_n^{\lambda_2} V_{\lambda_1-\lambda_2}$ for $\lambda_1 + \lambda_2 \geq 2$, so

$$p^{2\mu+1} \,\left|\, \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} \tilde{Q}_n^{\lambda_2} V_{\lambda_1-\lambda_2}\right. .$$

Similarly, $p^\mu \mid \tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n)$ for $\lambda_1 + \lambda_2 \geq 2$, so

$$p^{\mu+1} \,\left|\, \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} \tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}\right. .$$

Finally, if $\lambda_1 + \lambda_2 = 1$, then

$$W_{pn} \equiv \pm p R^{(p-1)n} W_n \pmod{p^{2\mu+1}} \quad \text{and} \quad \frac{C_{pn}}{C_n} \equiv p R^{(p-1)n} \pmod{p^{\mu+1}}.$$

We may then conclude that if $p^\mu \mid\mid E_n$, then $p^{\mu+1} \mid\mid E_{pn}$. □

Also, notice that if $p > 3$, $p \nmid E_n$ and $p \nmid \Delta$, then $p \nmid E_{pn}$. For if $p \nmid C_n$, then $\tilde{\Delta}_n = \Delta C_n^2$, so $p \nmid \tilde{\Delta}_n$, and thus $U_p(\tilde{P}_n, \tilde{Q}_n) \not\equiv 0 \pmod{p}$. But

$$\frac{C_{pn}}{C_n} \equiv U_p(\tilde{P}_n, \tilde{Q}_n) \pmod{p},$$

so $p \nmid C_{pn}$. Also, since, $p \mid W_n$ if and only if $p \mid W_{pn}$ whenever $p \mid C_n$, we see that $p \nmid E_{pn}$ when $p \nmid W_n$.

### 6.6. A law of apparition for $\{E_n\}$

It will be seen here that $\{E_n\}$ behaves in much the same way as $\{V_n\}$. By employing $\{E_n\}$, we will be able to extend more of the results for $\{V_n\}$ from Section 2 that were, until now, missing. We must first deal with the case of $p = 2$. Since $2 \mid E_n$ if and only if $2 \mid C_n$, from our results in Section 4.1 of [Roe09], there always exists some minimal $\rho$ such that $2 \mid E_\rho$ and $2 \mid E_n$ if and only if $\rho \mid n$. We next consider the case of a general modulus. We note by the first two identities in Corollary 4.8 that $C_n \mid C_{2n}$ and $W_{2n} \equiv (\Delta C_n^2 + W_n^2)/2 \pmod{W_n}$. Since $E_n$ is either odd or $2 \mid\mid E_n$, it is easy to see that $E_n \mid E_{2n}$.

The following theorem provides an analogue to Theorem 2.11.

**Theorem 6.18.** *Suppose that $r \mid E_n$, with $n > 0$. Then there must be a least positive $\rho = \rho(r)$ such that $r \mid E_\rho$. Further, $\rho \mid n$.*

### 6.7. Further observations on $\{E_n\}$

The next theorems parallel Theorems 2.12 and 2.13.

**Theorem 6.19.** *If $3^\mu \mid\mid m$, $3^\nu \mid\mid n$ and $\mu = \nu$, then*

$$gcd(E_m, E_n) = E_{gcd(m,n)}.$$

**Theorem 6.20.** *If $3^\mu \mid\mid m$, $3^\nu \mid\mid n$ and $\mu \neq \nu$, then*

$$gcd(E_m, E_n) \mid 6.$$

### 6.8. Euler's criterion for $\{D_n\}$ and $\{E_n\}$

We restate Euler's criterion for $U_n$, $V_n$ as follows.

**Theorem 6.21.** *If $p \nmid 2\Delta Q$, then*

$$\begin{cases} p \mid U_{\frac{T(p)}{2}} & \iff & Q^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \\ p \mid V_{\frac{T(p)}{2}} & \iff & Q^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \end{cases}$$

*where $T(p) = p - 1$ if $p$ splits in $\mathbb{Q}(\alpha)$, and $T(p) = p + 1$ otherwise.*

Our analogue of Euler's criterion for $D_n$ and $E_n$ is stated in the theorem below. The proof of the following theorem relies on results in Sections 4.5, 5.3 and 6.3 of [Roe09]. We first suppose that $p$ is a prime such that $p \nmid 6\Delta R$. Define $T = T(p)$ to be $p - 1$, $p^2 - 1$ or $p^2 + p + 1$ for $p$ an $S$ prime, a $Q$ prime or an $I$ prime, respectively.

**Theorem 6.22.** *The equivalence*

$$p \mid D_{\frac{T(p)}{3}} \iff R^{\frac{p-1}{3}} \equiv 1 \pmod{p},$$

*holds for any prime $p \equiv 1 \pmod{3}$, with the additional assumption that $p \mid C_{\frac{p-1}{3}}$ when $p$ is an $S$ prime. The equivalence*

$$p \mid E_{\frac{T(p)}{3}} \iff R^{\frac{p-1}{3}} \not\equiv 1 \pmod{p}$$

*holds for any $S$ or $Q$ prime $p \equiv 1 \pmod{3}$. If $p$, with $p \equiv 1 \pmod{3}$, is an $I$ prime, then $p \nmid E_{\frac{T(p)}{3}}$.*

# 7. Primality testing

## 7.1. An analogue of Lucas's fundamental theorem

As mentioned in Section 3, one of Lucas's main purposes in attempting to extend his functions was to find new primality tests. In this section we explore how the $W_n$ and $C_n$ functions can be used for producing such tests. We first develop some analogues of Theorem 2.16 of Section 2. We begin with a simple lemma.

**Lemma 7.1.** *If $k \geq 2$ and $r_i \geq 5$, for $i = 1, 2, \ldots, k$, then*

$$\left(\prod_{i=1}^{k} r_i^2\right) - 1 > 2\prod_{i=1}^{k}\left(\frac{r_i^2 + r_i + 1}{2}\right).$$

**Proof.** We note that

$$1 > \frac{1}{5^4} + 2\left(\frac{7}{10}\right)^2,$$

hence

$$1 > \frac{1}{5^{2k}} + 2\left(\frac{7}{10}\right)^k$$

for $k \geq 2$. Now

$$\frac{1}{5^{2k}} \geq \prod_{i=1}^{k}\frac{1}{r_i^2} \quad \text{and} \quad \frac{7}{5} = 1 + \frac{2}{5} > 1 + \frac{1}{r_i} + \frac{1}{r_i^2}$$

imply that

$$1 > \prod_{i=1}^{k}\frac{1}{r_i^2} + 2\prod_{i=1}^{k}\left(\frac{1 + \frac{1}{r_i} + \frac{1}{r_i^2}}{2}\right).$$

Therefore,

$$\left(\prod_{i=1}^{k} r_i^2\right) > \left(\prod_{i=1}^{k} r_i^2\right)\left(\prod_{i=1}^{k}\frac{1}{r_i^2}\right) + \left(\prod_{i=1}^{k} r_i^2\right)\left(2\prod_{i=1}^{k}\left(\frac{1 + \frac{1}{r_i} + \frac{1}{r_i^2}}{2}\right)\right)$$

and

$$\left(\prod_{i=1}^{k} r_i^2\right) - 1 > 2\prod_{i=1}^{k}\left(\frac{r_i^2 + r_i + 1}{2}\right). \qquad \square$$

**Theorem 7.2.** *Let $N$ be an integer such that $gcd(N, 6) = 1$. If $N \mid D_{N^2-1}$ and $N \nmid D_{\frac{N^2-1}{q}}$ for all primes $q$ such that $q \mid N^2 - 1$ and $gcd\left(D_{\frac{N^2-1}{q'}}, N\right) = 1$, for some prime divisor $q'$ of $N^2 - 1$, then $N$ is a prime.*

**Proof.** Clearly $\omega(N)$ exists and $\omega(N) \mid N^2 - 1$. Also, if $\omega(N) \neq N^2 - 1$, then $N^2 - 1 = k\omega(N)$, where $k > 1$. If $q$ is any divisor of $k$, then $\omega(N) \mid \frac{N^2-1}{q}$, so $N \mid D_{\frac{N^2-1}{q}}$, which is a contradiction. Hence $\omega(N) = N^2 - 1$. Let

$$N = \prod_{i=1}^{k} p_i^{\alpha_i},$$

where the primes $p_i$ are all distinct and exceed 4. Also, $N \mid D_{N^2-1}$, then by equation (17) and the fact that $2 \nmid N$, we must have $gcd(N, R) = 1$. We know by Theorem 6.8 that

$$\omega(N) = lcm[\omega(p_i^{\alpha_i}); i = 1, 2, \ldots, k].$$

Since $(p_i, \omega(N)) = 1$ and, by Theorem 6.7, $\omega(p_i^{\alpha_i}) = p_i^{\nu}\omega(p_i)$, we must have

$$\omega(N) \mid lcm[\omega(p_i); i = 1, 2, \ldots, k].$$

Let $p$ be a prime divisor of $N$. We have $p \mid D_{N^2-1}$ and $p \nmid D_{\frac{N^2-1}{q'}}$. Hence $\omega(p) \mid N^2-1$ and $\omega(p) \nmid \frac{N^2-1}{q'}$, so $q' \mid \omega(p)$. Hence

$$lcm[\omega(p_i); i = 1, 2, \ldots, k] \;\Bigg|\; q' \prod_{i=1}^{k} \frac{\omega(p_i)}{q'}.$$

Now, for $k \geq 2$ we have by Corollary 6.6,

$$q' \prod_{i=1}^{k} \frac{\omega(p_i)}{q'} \leq q' \prod_{i=1}^{k} \frac{p_i^2 + p_i + 1}{q'} \leq 2 \prod_{i=1}^{k} \frac{p_i^2 + p_i + 1}{2},$$

so we get

$$\left(\prod_{i=1}^{k} p_i^2\right) - 1 \leq N^2 - 1 \leq 2 \prod_{i=1}^{k} \frac{p_i^2 + p_i + 1}{2},$$

which is impossible by the previous lemma.

If $k = 1$, then $N = p^{\alpha}$ and by Theorem 6.7 $\omega(N) = \omega(p^{\alpha}) = p^{\nu}\omega(p)$, which implies $N^2 - 1 = \omega(p)$ since $gcd(p, N^2-1) = 1$. If $\alpha \geq 2$, then $p^4 - 1 \leq p^2 + p + 1$, which is a contradiction. Thus $N = p$, a prime. □

By similar methods used to prove the previous theorem we also have the following result.

**Theorem 7.3.** *Let $N$ be an integer such that $gcd(N, 6) = 1$. If $N \mid D_{N^2+N+1}$, $N \nmid D_{\frac{N^2+N+1}{q}}$ for each prime divisor $q$ of $N^2 + N + 1$, and $gcd\left(D_{\frac{N^2+N+1}{q'}}, N\right) = 1$ for some prime divisor $q'$ of $N^2 + N + 1$, then $N$ is a prime.*

We have proved our analogue of Theorem 2.16.

**Theorem 7.4.** *Let $N$ be an integer such that $gcd(N, 6) = 1$ and let $T = N^2 - 1$ or $T = N^2 + N + 1$. If $N \mid D_T$, $N \nmid D_{\frac{T}{q}}$ for each prime divisor $q$ of $T$, and $gcd\left(D_{\frac{T}{q'}}, N\right) = 1$ for some prime divisor $q'$ of $T$, then $N$ is a prime.*

The difficulty in providing this as a complete analogue to Lucas's result is the need to involve the prime $q'$, which is not needed in Theorem 2.16. This is because $2 \mid N \pm 1$ and $2 \mid p_i \pm 1$, and any proof of Theorem 2.16 makes use of these observations. In what follows, we will modify Theorems 7.2 and 7.3 to eliminate the need for $q'$ in certain cases.

Suppose $p$ is a prime such that $p \nmid 6\Delta$ and $3 \mid T(p)$. By Theorem 6.5 of [Roe09], we know that if $m = T(p)/3$, then $p \nmid C_m$ if and only if

$$W_m \equiv -3R^m \quad \text{and} \quad \Delta C_m^2 \equiv -27R^{2m} \pmod{p}.$$

We also have a result for an arbitrary modulus.

**Lemma 7.5.** *Let* $gcd(N,6) = 1$. *If* $\Delta C_n^2 \equiv -27R^{2n} \pmod{N}$ *and* $W_n \equiv -3R^n \pmod{N}$, *then* $N \mid D_{3n}$ *and* $N \nmid C_n$.

**Proof.** We have $\Delta C_n^2 + 3W_n^2 \equiv 0 \pmod{N}$. Since $4C_{3n} = C_n(\Delta C_n^2 + 3W_n^2)$, we get $N \mid C_{3n}$. Also, $4W_{3n} = 3\Delta C_n^2(W_n + 2R^n) + W_n^2(W_n - 6R^n) + 24R^{3n}$ implies

$$\begin{aligned}
4(W_{3n} - 6R^{3n}) &= 3\Delta C_n^2(W_n + 2R^n) + W_n^2(W_n - 6R^n) \\
&\equiv -9W_n^2(W_n + 2R^n) + W_n^2(W_n - 6R^n) \pmod{N} \\
&\equiv -9W_n^3 - 18R^nW_n^2 + W_n^3 - 6R^nW_n^2 \pmod{N} \\
&\equiv -8W_n^3 - 24R^nW_n^2 \pmod{N} \\
&\equiv -8W_n^2(W_n + 3R^n) \equiv 0 \pmod{N}.
\end{aligned}$$

Thus $N \mid W_{3n} - 6R^{3n}$, so $N \mid D_{3n}$. Now since $gcd(W_n, C_n, R) \mid 2$ by Theorem 5.3 and $gcd(N,6) = 1$, we have $gcd(N,R) = 1$, and then $N \nmid C_n$. □

We can use the last result to prove the following theorem.

**Theorem 7.6.** *Suppose* $N$ *is odd*, $3 \mid T(N)$, $\Delta C^2_{\frac{T(N)}{3}} \equiv -27R^{\frac{2T(N)}{3}} \pmod{N}$, $W_{\frac{T(N)}{3}} \equiv -3R^{\frac{T(N)}{3}} \pmod{N}$, *and* $N \nmid C_{\frac{T(N)}{q}}$ *for each prime divisor* $q$ *of* $\frac{T(N)}{3}$. *Then* $N$ *is a prime.*

**Proof.** By the previous lemma, we know that $N \mid D_{T(N)}$ and $N \nmid D_{\frac{T(N)}{q}}$ for all prime divisors of $T(N)$. By our earlier reasoning we have $\omega(N) = T(N)$. Also, since $gcd(T(N), N) = 1$,

$$\omega(N) = lcm[\omega(p_i); i = 1, 2, \ldots, k], \quad \text{if } N = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Let $p$ be any prime divisor of $N$. If $p \mid R$, then by the conditions of the theorem $p \mid W_{\frac{T(N)}{3}}$ and $p \mid \Delta C_{\frac{T(N)}{3}}$. Since $p \nmid C_{\frac{T(N)}{3}}$ by Lemma 7.5, we must have $p \mid \Delta$. However, it can be shown that if $gcd(Q,R) = 1$, then $gcd(W_n, R, \Delta) \mid 4$; thus we can only have $p = 2$, which is not possible because $N$ is odd. Thus, $gcd(N,R) = 1$. Also, if $p \mid N$ and $p \mid \Delta$, then $p \mid R$ and $p \mid W_{\frac{T(N)}{3}}$, which is also impossible. It follows that $gcd(N, 6\Delta R) = 1$. Now since $p \mid C_{T(N)}$ and $p \nmid C_{\frac{T(N)}{3}}$, we get

$$p \mid \Delta C^2_{\frac{T(N)}{3}} + 3W^2_{\frac{T(N)}{3}}$$

and we know that $p \nmid \Delta C_{\frac{T(N)}{3}} W_{\frac{T(N)}{3}}$. Thus $\left(\frac{-3\Delta}{p}\right) = 1$. If $p$ is an $I$ prime, then $\omega(p) \mid p^2 + p + 1$, $\left(\frac{\Delta}{p}\right) = 1$ and $\left(\frac{-3}{p}\right) = 1$, which means that $p \equiv 1 \pmod 3$ and $3 \mid p^2 + p + 1$. If $p$ is a $Q$ prime, then $\omega(p) \mid p^2 - 1$ and $3 \mid p^2 - 1$. If $p$ is an $S$ prime, then $\omega(p) \mid p - 1$ and $p - 1 < (p^2 - 1)/3 < (p^2 + p + 1)/3$. Thus,

$$lcm[\omega(p_i); i = 1, 2, \ldots, k] \leq 3 \prod_{i+1}^{k} \frac{p_i^2 + p_i + 1}{3}.$$

That $N$ is a prime now follows from our previous reasoning. □

Notice that $3 \,|T(N)$ when $T(N) = N^2 - 1$ and $3 \,|T(N)$ when $T(N) = N^2 + N + 1$ and $N \equiv 1 \pmod 3$.

A more general result than Theorem 7.6, and one that is more in line with Lucas's precept that the primality of $N$ can be established by showing that $N$ divides certain integers, is provided in Theorem 7.8 below. In order to demonstrate this result we need a simple lemma.

**Lemma 7.7.** *Suppose that $N$ is odd and let $m$ be any positive integer such that $gcd(m, N) = 1$. If $N \mid C_{mn}/C_n$, then $gcd(N, D_n) = 1$.*

**Proof.** Suppose $p$ is any prime divisor of $D_n$ and $N$. Since $p \,|C_n$ and $p \,|W_n - 6R^n$, we see by our results in Section 6.3, in particular equation (19), that we have

$$C_{mn}/C_n \equiv m^3 R^{n(m-1)} \pmod p.$$

It follows that since $p \nmid m$ and $p \nmid R$ ($gcd(D_n, R) \mid 2$), we must have $p \nmid C_{mn}/C_n$, contradicting $N \mid C_{mn}/C_n$. □

We are now able to produce an analogue of Corollary 2.18.

**Theorem 7.8.** *Let $N$ be an integer such that $gcd(N, 6) = 1$. If $N \mid D_{T(N)}$ and $N \left| \left( C_{T(N)}/C_{\frac{T(N)}{q}} \right) \right.$ for each prime divisor $q$ of $T(N)$, then $N$ is a prime.*

**Proof.** Since $gcd(T(N), N) = 1$, we have $gcd(q, N) = 1$. By Lemma 7.7 we know that if $p$ is any prime divisor of $N$, then $gcd\left(N, D_{\frac{T(N)}{q}}\right) = 1$. Thus, $N \nmid D_{\frac{T(N)}{q}}$ for all prime divisors $q$ of $T(N)$ and $gcd\left(N, D_{\frac{T(N)}{q'}}\right) = 1$ for any prime divisor $q'$ of $T(N)$. The result follows by Theorem 7.4. □

We note here that Lucas himself ([Luc78], pp. 310-311) made use of the divisibility of $U_{3n}/U_n$ to produce a primality test for $N = A3^n - 1$. Also, the computation of $C_T/C_{\frac{T}{q}}$ can be done efficiently by using the methods of Section 3.6 of [Roe09].

Unfortunately, results like Theorems 7.4 and 7.8 are of limited utility in primality testing because we need to know the complete factorization of $T(N)$, and this is often not available to us. In the next subsection, we will consider some special cases when $T(N) = N^2 + N + 1$.

### 7.2. The case of $T(N) = N^2 + N + 1$

We will deal here with the case of $N^2 + N + 1 = tL$, where $L$ is a prime.

**Theorem 7.9.** *Let $N^2 + N + 1 = tL$, where $L$ is a prime. If $t < N - \sqrt{N} + 1$, $(N, D_t) = 1$ and $N \mid D_{N^2+N+1}$, then $N$ is a prime.*

**Corollary 7.10.** *If $N$ is odd, $N \equiv 1 \pmod 3$, $L = (N^2 + N + 1)/3$ is a prime, $gcd(N, D_3) = 1$, and $N \mid D_{N^2+N+1}$, then $N$ is a prime.*

We also have the following result.

**Theorem 7.11.** *Let $N^2 + N + 1 = tL$, where $L$ is a prime. If $L > t^2 + t + 1$, $gcd(N, D_t) = 1$ and $N \mid D_{N^2+N+1}$, then $N$ is a prime.*

Now, suppose that $S$ is a fixed positive integer and $N = tS+u$, where $t = u^2+u+1$ and $u \in \mathbb{Z}$. Then $N^2 + N + 1 = tL$, where

$$L = tS^2 + (2u + 1)S + 1.$$

For such numbers, we have the following result.

**Theorem 7.12.** *If $N = tS+u$, where $S \geq 2$ and $N > 4$, we have $t < N-\sqrt{N}+1$.*

From Theorems 7.9 and 7.12 we see that if $tS^2 + (2u+1)S + 1$ is a prime, then we can use the test of Theorem 7.9 to prove that $tS+u$ is a prime. Of course, if $N = tS+u$ is a prime, it might not be an $I$ prime and therefore $T(N) \neq N^2+N+1$; consequently, this test would not be successful. Thus, we need to find values for $P$, $Q$ and $R$ such that if $N = tS + u$ is a prime, then $N$ is an $I$ prime for $f(x) = x^3 - Px^2 + Qx - R$. It is well-known (see [Wil72b] and [Leh58]) that if $N$ is a prime and

$$N^{\frac{p-1}{3}} \not\equiv 1 \pmod p,$$

where $p$ is a prime (equivalent to 1 modulo 3), $4p = r^2 + 27s^2$ with $r \equiv 1 \pmod 3$ and $N \nmid spr$, then the cubic congruence

$$x^3 - 3px - pr \equiv 0 \pmod N$$

is irreducible; that is, $N$ is an $I$ prime for

$$P \equiv 0, \quad Q \equiv -3p \quad \text{and} \quad R \equiv pr \pmod N.$$

Notice that since $gcd(pr, N) = 1$, there always exists some $x$ such that

$$gcd(pr + xN, -3p) = 1;$$

hence, the fact that $gcd(-3p, pr) = p \neq 1$ does not have any effect on the validity of our results. We have proved the following theorem.

**Theorem 7.13.** *Let $L = tS^2 + (2u + 1)S + 1$ be a prime and put $N = tS + u$. Suppose that $(N, 6) = 1$, $p$ is a prime such that $p \equiv 1 \pmod 3$, $N^{\frac{p-1}{3}} \not\equiv 1 \pmod p$ and $4p = r^2 + 27s^2$, with $r \equiv 1 \pmod 3$ and $gcd(N, prs) = 1$. If we put*

$$P \equiv 0, \quad Q \equiv -3p \quad \textit{and} \quad R \equiv pr \pmod N,$$

*then $N$ is a prime if and only if $N \mid D_{N^2+N+1}$ and $gcd(D_t, N) = 1$.*

**Corollary 7.14.** *Let $2 \nmid S$, and $L = 3S^2 - 3S + 1$ be a prime. Suppose that $p$ is a prime such that $p \equiv 1 \pmod 3$ and*

$$N^{\frac{p-1}{3}} \not\equiv 1 \pmod p,$$

*where $N = 3S - 2$. If we define $r$ and $s$ as above and $gcd(N, prs) = 1$, then $N$ is a prime if and only if $N \mid D_{N^2+N+1}$, where*

$$P \equiv 0, \;\; Q \equiv -3p \text{ and } R \equiv pr \pmod N.$$

Notice that we need only perform $O(\log N(M(\log_2 N)))$ operations to establish the primality of $N$, once we know that $L$ is a prime. (Here we use $M(n)$ to denote the number of elementary bit operations needed to multiply two $n$-bit integers.) This is much faster than several other tests because it is not necessarily all that easy to find enough factors of $N \pm 1$ to use the techniques of Brillhart, Lehmer and Selfridge [BLS75], which generalized those of Lucas, to establish the primality of $N$.

### 7.3. The primality of *L*

If we put

$$L = tS^2 + (2u + 1)S + 1, \;\; t = u^2 + u + 1 \quad \text{and} \quad N = tS + u,$$

the results of the last section allow us to establish the primality of $N$, when we have already proved $L$ is a prime. This is not a vacuous result because we certainly expect by the Bateman–Horn conjecture [BH62] that there exists an infinitude of values of $S$ such that for a fixed $u$, $L$ and $N$ will both be prime. Also, for a fixed value of $S$, we would expect that there exists an infinitude of values of $u$ such that both $L$ and $N$ will be prime. There remains, however, the difficulty of proving that $L$ is a prime. We notice, however, that $S \mid L - 1$. Suppose that $S = FG$, where we know the complete factorization of $F$. It is then possible, by using the methods of [BLS75] to prove that $L$ is either prime or that all the prime factors of $L$ must have the form $kF + 1$.

**Theorem 7.15.** *Suppose that $L = tS^2 + (2u + 1)S + 1$ (with $t = u^2 + u + 1$), $S = FG$ and all the prime factors of $L$ have the form $kF + 1$. Then $L$ is a prime whenever $F > tG^2 + |2u + 1|G + 2$.*

Suppose that we now consider the simple example where we put $F = 2^n$, $G = 1$. We get

$$L_n = (u^2 + u + 1)2^{2n} + (2u + 1)2^n + 1, \;\; \text{and} \;\; N_n = (u^2 + u + 1)2^n + u.$$

In this case, if $2^n > u^2 + 3|u| + 4$, we can easily establish (when it is the case) that $L_n$ is a prime. We can next use our earlier results to prove that $N_n$ is a prime, when that is the case. This is not a vacuous result as both $L_n$ and $N_n$ are prime for $n = 819$ and $u = 289$.

If we put $F = q^n$, where $q$ is a prime and $G = 1$, we can once again easily establish the primality of

$$L_n = (u^2 + u + 1)q^{2n} + (2u + 1)q^n + 1$$

when $L_n$ is a prime. However, if we specify $q$ and $u$, it seems a very rare event to have both $L_n$ and $N_n = (u^2 + u + 1)q^n + u$ prime simultaneously. In the particular case where $u = -2$ and $q = 3$ we get

$$L_n = 3^{2n+1} - 3^{n+1} + 1 \quad \text{and} \quad N_n = 3^{n+1} - 2.$$

For $n > 3$, we need only find some $b$ such that

$$(21) \qquad b^{L_n - 1} \equiv 1 \pmod{L_n} \quad \text{and} \quad gcd\left(b^{\frac{L_n-1}{3}} - 1, L_n\right) = 1,$$

to establish that $L_n$ is a prime. Note that $3^{n+1} \mid\mid L_n - 1$. Suppose $p$ is some prime such that $p \mid L_n$. By (21) we have

$$p \mid b^{L_n-1} - 1 \quad \text{and} \quad p \nmid b^{\frac{L_n-1}{3}} - 1.$$

If $\omega$ is the order of $b$ modulo $p$, then

$$\omega \mid L_n - 1 \quad \text{and} \quad \omega \nmid \frac{L_n - 1}{3}.$$

So $3^{n+1} \mid \omega$ and $\omega \mid p - 1$; thus $p \equiv 1 \pmod{3^{n+1}}$. Hence $p = k3^{n+1} + 1$ for some $k \in \mathbb{N}$. We then have $p \geq 2 \cdot 3^{n+1} + 1$ and we can conclude that $L_n$ is a prime since $p > \sqrt{L_n}$. Having done this we can use Corollary 7.14 to establish that $N_n$ is a prime. This sort of testing of pairs of numbers for primality might have pleased Lucas.

## 7.4. The case of $T(N) = N^2 - 1$

It is certainly possible to test numbers of the form $Aq^n \pm 1$ for primality by using the $W_n$ and $C_n$ functions; however, we will confine our attention here to the case where $N = A3^n - 1$, as this is the analogous form to $A2^n - 1$ mentioned in Chapter 2. We can produce a theorem similar to Theorem 2.19, except for the necessity condition.

**Theorem 7.16.** *Let $N = A3^n - 1$, where $2 \mid A$, $A < 3^n$, $n \geq 2$ and $gcd(N, R) = 1$. If $N \mid \left(C_{N+1}/C_{\frac{N+1}{3}}\right)$, then $N$ is prime.*

Our next objective will be to produce conditions that are both necessary and sufficient for $N = A3^n - 1$ to be prime. We first need to produce a result analogous to Theorem 2.21. We begin with the following theorem.

**Theorem 7.17.** *Let $p$ be an odd prime such that $p \equiv -1 \pmod 3$. Then there exist $P$, $Q$ and $R$ such that $p$ is a $Q$ prime if and only if*

$$P \equiv a + Tr(\lambda), \quad Q \equiv aTr(\lambda) + N(\lambda) \ \textit{and} \ R \equiv aN(\lambda) \pmod p,$$

*where $a \in \mathbb{Z}$, $\lambda = r_1 + r_2\rho \in \mathbb{Z}[\rho]$, $\rho^2 + \rho + 1 = 0$ and $p \nmid ar_2N(\lambda)$.*

We can now present our analogue of Theorem 2.21.

**Theorem 7.18.** *Let $p$ be an odd prime such that $p \equiv -1 \pmod 3$. If $P$, $Q$ and $R$ satisfy the conditions of Theorem 7.17 and $\left(\frac{\lambda}{p}\right)_3 \neq 1$, then*

$$p \left| \left(C_{p+1}/C_{\frac{p+1}{3}}\right)\right. .$$

By combining Theorems 7.16 and 7.18 we get the following necessary and sufficient condition for $N = A3^n - 1$, with $2 \mid A$ and $A < 3^n$, to be prime.

**Theorem 7.19.** *Let $N = A3^n - 1$, where $2 \mid A$ and $3 < A < 3^n$. Futhermore, let $q \equiv 1 \pmod 3$ be a prime such that $q \nmid N$ and*

$$N^{\frac{q-1}{3}} \not\equiv 1 \pmod q.$$

*Let* $\lambda = r_1 + r_2\rho$*, with* $\rho^2 + \rho + 1 = 0$*, be a primary prime divisor of* $q$ *in* $\mathbb{Z}[\rho]$ *and suppose that* $N \nmid r_2$*. Let*

$$P \equiv a + Tr(\lambda), \quad Q \equiv aTr(\lambda) + q, \quad \text{and} \quad R \equiv aq \pmod{N},$$

*where* $(a, N) = 1$*. Then* $N$ *is a prime if and only if*

$$N \;\Big|\; \left(C_{p+1}/C_{\frac{p+1}{3}}\right).$$

## 8. Conclusion

The purpose of this research was to develop a cubic extension of the Lucas functions that Lucas himself might have discovered. What has emerged from this work is a theory of two functions that displays a number of pleasing similarities with Lucas's original work. The main tools in Lucas's investigation of his functions were the multiplication formulas (13) and (14). The multiplication formulas, proved in Subsection 4.5, allowed us to obtain arithmetic results that closely resemble those for the Lucas case. Key results like the laws of repetition and apparition, and Euler's criterion, have analogues in our extension. Most remarkably, the extension relies on the use of only two functions, despite the fact that you would expect three for the cubic case. (It might be argued that we are really considering four functions here because of $D_n$ and $E_n$, but these latter functions are simply a convenient way of representing certain divisors of $C_n$.) Further, when restricted to the quadratic case, our generalization in Section 4.3 satisfyingly reduces to that of Lucas sequences.

With all that in mind, it is difficult to point to a single "main" result. However, knowing that Lucas's own goal in generalizing his sequences was to find and implement new primality tests, Theorem 7.19 stands out as we can easily implement a primality test based on it. The test makes use of $\{C_n\}$, a sequence known to Lucas that surely would have been a part of any generalization he would have done, to test numbers of the form $A3^n - 1$. Certainly, even more important than just the primality test is Theorem 7.4, a result that is our analogue of Theorem 2.16, which Lucas refered to as his fundamental theorem. It should be emphasized, however, that today there exist many sophisticated methods for primality proving (see, for example, Chapter 4 of [CP01]). The primality conditions proved here are of mere historical interest and are perhaps what Lucas had in mind.

*Acknowledgments.* The authors gratefully acknowledge the work of an anonymous referee, whose many helpful comments caused us to produce a much better version of this paper than the one originally submitted. The third author was supported by NSERC of Canada and iCORE of Alberta.

## References

[AS82] W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), no. 159, 255–300.

[Bal95] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995), no. 551, viii+102 pp.

[Bal99] C. Ballot, *Strong arithmetic properties of the integral solutions of $X^3+DY^3+D^2Z^3-3DXYZ=1$, where $D=M^3\pm 1, M\in\mathbb{Z}^*$*, Acta Arith. **89** (1999), no. 3, 259–277.

[BH62] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962) 363–367.

[Bel24] E. T. Bell, *Notes on recurring series of third order*, Tôhoku Math. J. **24** (1924), 168–184.

[BLS75] 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.

[Car13] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n\pm\beta^n$*, Ann. of Math. (2) **15** (1913/14), no. 1-4, 30–70.

[Car20] R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quart. J. Math. Oxford Ser. **48** (1920), 343–372.

[CP01] R. Crandall and C. Pomerance, *Prime numbers*, A computational perspective, Springer-Verlag, New York, 2001, xvi+545 pp.

[Déc99] A. M. Décaillot–Laulagnet, *Édouard Lucas (1842-1891): le parcours original d'un scientifique français dans la deuxième moitié du XIX-ième siècle*, Ph.D. thesis, Université René Descartes - Paris V, 1999.

[dL80] M. G. de Longchamps, *Sur les fonctions récurrentes du troisième degré*, AFAS **9**th (1880), 115–117.

[DLL95] H. Delannoy, C.-A. Laisant and E. Lemoine, *Question 177*, L'Intermédiaire des Mathématiciens **2** (1895), 341.

[Dic19] L. E. Dickson, *History of the theory of numbers*, Carnegie Institution of Washington, Publication No. **256** (1919).

[Eng31] H. T. Engstrom, *On sequences defined by linear recurrence relations*, Trans. Amer. Math. Soc. **33** (1931), no. 1, 210–218.

[Har57] D. Harkin, *On the mathematical work of François-Édouard-Anatole Lucas*, L'Enseignement Math. (2) **3** (1957), 276–288.

[Lai96] C.-A. Laisant, *Question 744*, L'Intermédiaire des Mathématiciens **3** (1896), 33–34.

[Laz07] D. Lazzeri, *Gastone Gohierre de Longchamps*, Periodico di matematica **4** (1907), 53–59.

[Leh27] D. H. Lehmer, *Tests for primality by the converse of Fermat's theorem*, Bull. Amer. Math. Soc. **33** (1927), no. 3, 327–340.

[Leh30] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), no. 3, 419–448.

[Leh35] D. H. Lehmer, *On Lucas's test for the primality of Mersenne's numbers*, J. London Math. Soc. **10** (1935), 162–165.

[Leh58] E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.

[Luc76] E. Lucas, *Sur les rapports qui existent entre la théorie des nombres et le calcul intégral*, Comptes Rendus Acad. des Sciences, Paris **82** (1876), 1303–1305.

[Luc78] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 189–240, 289–321.

[Luc80] E. Lucas, *Notice sur les titres et travaux scientifiques de M. Édouard Lucas*, D. Jouaust, Paris, 1880.

[Luc91a] E. Lucas, *Questions proposées à la discussion des 1re et 2e sections* $1^o$ *questions d'arithmétique supérieure*, Assoc. Française pour l'Avancement des Sciences, Compte rendu des sessions **20** (1891), 149–151.

[Luc91b] E. Lucas, *Théorie des nombres*, Gauthier-Villars, Paris, 1891.

[Mac15] P. A. MacMahon, *Combinatory analysis*, vol. I, Chelsea Publishing Company, 1915.

[Men62] N. S. Mendelsohn, *Congruence relationships for integral recurrences*, Canad. Math. Bull. **5** (1962), 281–284.

[Mül01] S. Müller, *On the rank of appearance and the number of zeros of the Lucas sequences over* $\mathbf{F}_q$, Finite Fields and Applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 390–408.

[Mül04] S. Müller, *On the computation of cube roots modulo* $p$, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, 293–304, Fields Inst. Commun., **41**, Amer. Math. Soc., Providence, RI, 2004.

[Rib89] P. Ribenboim, *The book of prime number records*, Second edition, Springer-Verlag, New York, 1989. xxiv+479 pp.

[Roe09] E. Roettger, *A cubic extension of the Lucas functions*, Ph.D. thesis, University of Calgary, 2009.

[Ser79] J.-A. Serret, *Cours d'algèbre supérieure. Tome II.*, Reprint of the fourth (1879) edition, Les Grands Classiques Gauthier-Villars, Éditions Jacques Gabay, Sceaux, 1992, xii+695 pp.

[War31a] M. Ward, *The algebra of recurring series*, Ann. of Math. (2) **32** (1931), no. 1, 1–9.

[War31b] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), no. 1, 153–165.

[War31c] M. Ward, *The distribution of residues in a sequence satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), no. 1, 166–190.

[War33] M. Ward, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. **35** (1933), no. 3, 600–628.

[War36] M. Ward, *A Calculus of Sequences*, Amer. J. Math. **58** (1936), no. 2, 255–266.

[War37] M. Ward, *Linear divisibility sequences*, Trans. Amer. Math. Soc. **41** (1937), no. 2, 276–286.

[War55] M. Ward, *The laws of apparition and repetition of primes in a cubic recurrence*, Trans. Amer. Math. Soc. **79** (1955), 72–90.

[Wil69] H. C. Williams, *A generalization of the Lucas functions*, Ph.D. thesis, University of Waterloo, 1969.

[Wil72a] H. C. Williams, *On a generalization of the Lucas functions*, Acta Arith. **20** (1972), 33–51.

[Wil72b] H. C. Williams, *The primality of* $N = 2A3^n - 1$, Canad. Math. Bull. **15** (1972), 585–589.

[Wil76] H. C. Williams, *A generalization of Lehmer's functions*, Acta Arith. **29** (1976), no. 4, 315–341.

[Wil77] H. C. Williams, *Properties of some functions similar to Lucas functions*, Fibonacci Quart. **15** (1977), no. 2, 97–112.

[Wil98] H. C. Williams, *Édouard Lucas and primality testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, **22**, A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998, x+525 pp.

[WZ74] H. C. Williams and C. R. Zarnke, *Some algorithms for solving a cubic congruence modulo $p$*, Utilitas Math. **6** (1974), 285–306.

S. MÜLLER, DEPT. OF MATHEMATICS AND STATISTICS, U. OF WYOMING, LARAMIE, WY 82071-3036, UNITED STATES.
smuller@uwyo.edu

E. ROETTGER, DEPT. OF MATHEMATICS, PHYSICS AND ENGINEERING, MOUNT ROYAL U., CALGARY, ALBERTA, CANADA, T3E 6K6.
eroettger@mtroyal.ca

H. C. WILLIAMS, DEPT. OF MATHEMATICS AND STATISTICS, U. OF CALGARY, 2500 UNIVERSITY DRIVE NW, CALGARY, ALBERTA, CANADA, T2N 1N4.
williams@math.ucalgary.ca