THE UNIVERSITY OF CALGARY

A Cubic Extension of the Lucas Functions

by

Eric L. F. Roettger

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

January, 2009

THE UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "A Cubic Extension of the Lucas Functions" submitted by Eric L. F. Roettger in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY.

Supervisor, Dr. H. C. Williams
Dept. of Mathematics and Statistics

Dr. R. Scheidler
Dept. of Mathematics and Statistics

Co–Supervisor, Dr. S. Müller
Dept. of Mathematics and Statistics
University of Wyoming

Dr. M. Bauer
Dept. of Mathematics and Statistics

Dr. W. Tittel
Dept. of Physics and Astronomy

Dr. C. Ballot
Laboratoire Nicolas Oresme
Université de Caen

Date

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 succeeded in demonstrating that the Mersenne number $2^{127} - 1$ is a prime. 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. Indeed, at the end of his life he stated that "by searching for the addition formulas of the numerical functions which originate from recurrence sequences of the third or fourth degree, and by studying in a general way the laws of residues of these functions for prime moduli... we would arrive at important new properties of prime numbers."

In this thesis we discuss a pair of functions that are easily expressed as certain symmetric polynomials of the zeros of a cubic polynomial and were undoubtedly known to Lucas. 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' 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.

Acknowledgments

I am endlessly indebted to my supervisor Dr. H. C. Williams. Without him I have no doubt this thesis would never have been completed. Beyond his valuable criticism throughout the writing of this thesis (and the endless rounds of corrections), Hugh provided me with much-needed guidance and counsel in all parts of my life. He also provided me with a considerable amount of money through the years, for which I am also properly grateful. I can sincerely say that no student has ever had a better supervisor than I.

Thanks to my co-supervisor Dr. Siguna Müller, for her encouragement and for providing me with such a remarkable thesis topic. Many thanks to my committee members, Dr. Christian Ballot, Dr. Mark Bauer, Dr. Renate Scheidler, and Dr. Wolfgang Tittel for the time they invested in reading my thesis and suggesting changes.

I would like to thank and acknowledge the Natural Sciences and Engineering Research Council of Canada for funding received. Thanks also to the Faculty of Graduate Studies and the entire Department of Mathematics at the University of Calgary.

Many thanks to my colleagues at the University of Calgary Mathematics Department: Aaron Christie, for his proofreading; to Pieter Rozenhart, my office mate who always helped me solve elementary number theory problems; Alan Silvester, who is a LaTeXwizard; and finally Kjell Wooding, who I must thank for all the conversations we had over beer or, to a lesser extent, over coffee.

Finally, I owe thanks to my family. My father Joe, mother Shirley, sister Jennelle, and brother David. I thank them for their support throughout this entire venture.

Table of Contents

Chapter 1

The Problem

1.1 Introduction

Let P and Q be coprime integers and α, β be the zeros of the polynomial $f(x) = x^2 - Px + Q$ where $\alpha \neq P$. The Lucas functions U_n and V_n are defined by:

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta), \quad V_n = \alpha^n + \beta^n.$$

Since both U_n and V_n are symmetric functions of the zeros of a polynomial with integer coefficients they must be integers for all non-negative integral values of n. Furthermore, they must both satisfy the simple linear recurrence:

$$X_{n+1} = PX_n - QX_{n-1}.$$

Since $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$, this recurrence can be used to compute U_n and V_n for any integral value of n.

From 1876 until about 1880, Édouard Lucas discovered many properties of these functions. Indeed, it was during this period that he used these properties to develop tests for the primality of large integers, including what is now called the Lucas-Lehmer test for the primality of Mersenne numbers. (See section 5.4 of [Wil98].) 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 test were quite novel for their time, because instead of having to trial 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 $N \mid S$.

It is important to recognize, however, that Lucas found many other applications of his functions. He was particularly struck by the similarity of his functions with the sine and cosine functions; in fact, he noticed that if i is used to denote a zero of $x^2 + 1$, then

$$U_n = (2Q^{n/2}/\sqrt{-\Delta}) \sin[(ni/2) \log(\alpha/\beta)] \quad \text{and} \tag{1.1}$$

$$V_n = 2Q^{n/2} \cos[(ni/2) \log(\alpha/\beta)], \tag{1.2}$$

where $\Delta = (\alpha - \beta)^2 = P^2 - 4Q$. As both sine and cosine are singly periodic functions with period 2π, Lucas (see Section 26 of [Luc78]) regarded U_n and V_n as simply periodic numerical functions, where for any particular modulus m, the (numerical) period in this case is the least positive integer p such that both

$$U_{n+p} \equiv U_n \pmod{m} \quad \text{and} \quad V_{n+p} \equiv V_n \pmod{m}$$

hold.

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. The purpose of this thesis is to provide an extension of the Lucas functions which makes use of the zeros of a cubic polynomial and to develop a theory which is very much analogous to that of the Lucas functions. The functions that we will discuss were almost certainly known to Lucas and the techniques that we will employ would have

been available to him; thus, it is conceivable that he might have developed some or much of this theory himself. However, we must emphasize here that the evidence that Lucas was thinking exactly along these lines is at best circumstantial.

1.2 Sources

In much of his published work on the U_n and V_n functions, Lucas mentioned the problem of extending or generalizing them. In what follows, we present the most important quotes, which are relevant to this theme. It should be pointed out that Lucas frequently repeated himself, so we will give only one of any repeated statements.

The first of these comes from [Luc76].

> *The objective that we intend in this note is to show the identity of formulas concerning certain numerical functions of the roots of an equation of the second degree with rational coefficients with those which connect to the circular functions, and to indicate, more generally, the identity of formulas concerning the numerical functions of the roots of an algebraic equation of the fourth or any degree with those which connect to the elliptic or abelian transcendentals.*

In his memoir [Luc78], the most extensive and important work which Lucas devoted to the Lucas functions, we have several interesting quotes.

> *This memoir has as its objective the study of symmetric functions of the roots of an equation of the second degree, and its application to the theory of prime numbers. We will first show the complete analogy of these symmetric functions with the circular and hyperbolic functions. We then show*

the connection that exists between the symmetric functions and the theory of determinants, combinations, continued fractions, divisibility, divisors of quadratic forms, continued radicands, division of the circumference of the circle, indeterminate analysis of the second degree, quadratic residues, decomposition of large numbers into their prime factors, etc. This method is the point of departure of a more complete study, of the properties of the symmetric functions of the roots of an algebraic equation of any degree with rational coefficients, in their relation to the theories of elliptic and Abelian functions, of power residues, and indeterminate analysis of higher degrees. (Section 1)

We will complete this section with the proof of formulas of extreme importance, because these will serve later as a basis for the theory of the numerical functions of double period, derived from the consideration of the symmetric functions of the roots of third and fourth degree equations with rational coefficients. (Section 9)

We see that the coefficients of the binomial raised to the power p are integers and divisible by p, whenever p denotes a prime number, except for the coefficients of the pth powers. On denoting by α, β, γ, $\ldots\lambda$, any n integers one has therefore

$$[\alpha+\beta+\gamma+\cdots+\lambda]^p-[\alpha^p+\beta^p+\gamma^p+\cdots+\lambda^p]\equiv 0 \pmod{p},$$

and, for $\alpha=\beta=\gamma=\cdots=\lambda=1$, one obtains

$$n^p-n\equiv 0 \pmod{p}.$$

It is this congruence which contains Fermat's theorem that one can generalize in the following manner, which is different from Euler's approach. If α, β, γ, $\ldots\lambda$, *denote the* q*th powers of the roots of an equation with integral coefficients, and* S_q *their sum, the first part of the preceding congruence represents the product by* p *of a symmetric function, integral and with integral coefficients, of the roots, and, as a consequence of the coefficients of the proposed equation. One has therefore*

$$S_{pq} \equiv S_q^p \pmod{p},$$

and by applying the Theorem of Fermat,

$$S_{pq} \equiv S_q \pmod{p}.$$

The study of the prime divisors of the numerical function S_n *and of some others which are analogous is very important; one has in particular, for* $n = 1$ *and* $S_1 = 0$, *as in the equation*

$$x^3 = x + 1,$$

the congruence

$$S_p \equiv 0 \pmod{p};$$

and thence deduces conversely that if, in the case of $S_1 = 0$, *one has* S_n *divisible by* p *for* $n = p$ *and not previously, the number* p *is prime. Indeed, suppose* p *is equal, for example, to the product of two primes* g *and* h. *One has*

$$S_{gh} \equiv S_h \pmod{g}$$

$$S_{gh} \equiv S_g \pmod{h};$$

as a consequence, if one finds that

$$S_{gh} \equiv 0 \pmod{gh},$$

one will also have

$$S_g \equiv 0 \pmod{h},$$
$$S_h \equiv 0 \pmod{g},$$

and, by the demonstrated theorem,

$$S_g \equiv S_h \equiv 0 \pmod{gh}.$$

Thus S_{gh} would not be the first of the numbers S_n divisible by gh. One can obtain, in this fashion, a great many theorems serving, like that of Wilson, to verify prime numbers. We will leave aside, for the moment, the curious and new developments that we have thus found, in order to consider only those which are derived from simply periodic numerical functions. (Section 21)

We have further indicated (Sections 9 and 21) a first generalization of the principal idea of this memoir in the study of recurrence sequences which arise from the symmetric functions of the roots of algebraic equations of the third and fourth degree and, more generally, of the roots of equations of any degree with rational coefficients. One finds, in particular, in the study of the function

$$U_n = \Delta(a^n, b^n, c^n, \dots)/\Delta(a, b, c, \dots)$$

> *in which a, b, c designate the roots of the equation, and $\Delta(a, b, c, \dots)$, the alternating function of the roots, or the square root of the discriminant of the equation, the generalization of the principal formulas contained in the first part of this work. (Section 29)*

In later writing concerning this memoir, Lucas [Luc80] remarked,

> *Since the publication of this work, the author has added to it twenty other sections, as yet unpublished, which altogether form the arithmetical theory of the symmetric functions of the roots of equations of the second degree. The author hopes to find the time to write up in a similar manner the theory of doubly periodic functions, in their connection to symmetric functions of the roots of equations of the third and fourth degree, and with elliptic functions.*

Finally, in the year of his death, Lucas [Luc91a] wrote at much greater length concerning the problem of generalizing his functions.

> *But we think that we should stress in particular research concerning linear recurring sequences of various orders and its connection to the theory of elliptic and abelian functions. In several papers published in the* Comptes rendues de l'association, *from the meetings in Clermont, Nancy, Paris and le Havre, in the* Actes de l'Académie royale des Sciences de Turin *and of Saint Petersburg, in* Nouvelle Correspondance mathématique, *in the* Journal de Sylvester *in Baltimore [American Journal of Mathematics], etc., we have demonstrated the analogy and,*

as it were, the identity of the circular and hyperbolic functions with the numerical functions of the second order, whose characteristic polynomials are of degree two. (See Chapters 17 and 18 in our book.) To every trigonometric formula corresponds a formula for these functions, and conversely.

We had hoped to find in this study, through the prime decomposition of the expressions $(a^n \pm b^n)$*, a demonstration of Fermat's last theorem concerning the impossibility of solving in integers the indeterminate equation*

$$x^p + y^p + z^p = 0$$

in which it suffices to assume that p *denotes a prime. Although Kummer treated this equation masterfully some time ago, it has still not been completely solved, since many of the exponents* p *cannot be dealt with by his admirable analysis.*

But if this research plan has not up to now provided the solution of this celebrated problem, it does allow us to obtain a number of Wilsonian *theorems, that is to say the necessary and sufficient conditions that a given* p *of twenty or thirty digits must satisfy to be prime when one knows the decomposition in prime factors of one of the numbers* $p \pm 1$*. Furthermore, this method guides us to the notion of periodicity of the residues for prime or composite moduli. Therefore, there is every reason to search for formulas analogous to the addition and multiplication formulas for the numerical functions which are derived from recurrences whose characteristic polynomials are of degree three and four. These formulas find*

their origin in the theory of elliptic functions, and we encounter some of them in a beautiful memoir of Moutard.

One rediscovers these recurrence sequences by generalizing the theory of linear substitutions, described by Serret in his Cours d'Algèbre supérieure *(4th edition, vol II, pp. 356-412) in a very particular form. If one considers n linear homogeneous forms in n variables provided by the linear substitutions in which the coefficients* λ, μ, ν, ..., *are constants, the forms* x_{p+1}, y_{p+1}, z_{p+1}, ..., *are expressed as functions of* x, y, z, ..., *and the coefficients of the variables* x, y, z, ..., *this produces a sequence of linear recurrences having for their characteristic equation*

$$U = \begin{vmatrix} \lambda_1 - u & \mu_1 & \nu_1 & \dots \\ \lambda_2 & \mu_2 - u & \nu_2 & \dots \\ \lambda_3 & \mu_3 & \nu_3 - u & \dots \\ \vdots & \vdots & \vdots & \ddots \end{vmatrix} = 0$$

where u denotes the variable. The ratios of consecutive functions, or of coefficients corresponding to two consecutive functions, have for their limits under certain conditions of convergence, the root of largest modulus of the equation $U = 0$. *One can therefore generalize in an infinitude of ways Bernoulli's approximation technique for calculating the roots of equations. This method is developed in the first volume of Legendre's* Théorie des nombres, *but only for a very particular case.*

In Addition X Sur l'extraction des racines pour les moyennes *(p. 506) of our book, we have pointed out a new process for obtaining roots of any*

index.

Furthermore, this process relates to the preceding theories and to linear substitutions. We think that, by developing these new methods, by searching for the addition and multiplication formulas of the numerical functions which originate from recurrence sequences of the third and of the fourth degree, and by studying in a general way the laws of the residues of these functions for prime moduli, according to their aspect, their character (cubic or biquadratic) for the discriminant of the equation $U = 0$, that we would arrive at important new properties of prime numbers. And perhaps the complete proof of Fermat's last theorem is just a consequence of the famous theorem of Jacobi concerning the impossibility of more than two periods for holomorphic functions of a single complex variable.

This is pretty much all that has survived of Lucas' writings on this problem. He may have been contemplating doing more in later volumes of his book, *Théorie des nombres* [Luc91b], only the first volume of which he completed (see Chapter 6 of [Déc99]), but there is little evidence to suggest this. However, in the introduction to this book, he wrote,

The theory of recurrent sequences is an inexhaustible mine which contains all the properties of numbers; by calculating the successive terms of such sequences, decomposing them into their prime factors and seeking out by experimentation the laws of appearance and reproduction of the prime numbers, one can advance in a systematic manner the study of the

> *properties of numbers and their application to all branches of mathematics.*

After Lucas' untimely death, there seemed to be little interest in the problem of generalizing his functions. His old friend, C.-A. Laisant tried to kindle some interest through a question in *L'Intermédiaire des mathématiciens* [Lai96].

> *We know how much the famous theorem of Fermat concerning the impossibility of the identity $x^n + y^n = z^n$, in integers, has so preoccupied mathematicians. We can no longer ignore that the greater part of the work of Éd. Lucas on the theory of numbers had for its object, direct or indirect, the quest for a demonstration of this theorem. In particular, he published a very interesting memoir* Sur la théorie des fonctions numériques simplement périodiques. *These functions U_n and V_n arise from the equation of the second degree and present striking analogies with the sine and cosine functions.*
>
> *In seeking to generalize these ideas, Lucas later sent a Communication to the* Société mathématique de France, *which unfortunately was not inserted, no Note having been put in by the author, on three numerical functions, arising from the equation of the third degree, offering very great analogies with the elliptic functions, and exhibiting the property of being doubly periodic.*
>
> *Shortly after, during a conversation that I had with him, Lucas said to me: "if one could establish that my doubly periodic functions only have two distinct periods, the theorem of Fermat would be proved." And*

> *during a meeting, assuming this hypothesis, he justified his statement by a demonstration which was easy for me to follow, but of which I have totally lost any memory, being far from suspecting his approaching death. I recall only that the case of the exponent 2 was isolated, just as it should be, in a very precise manner.*
>
> *It is possible that Lucas had made similar Communications to other colleagues, more favoured from the point of view of memory and more attentive than I had been. In this case, I make an appeal to them through the present question to consult their memories. It may also be possible that the members of the* Société mathématique *might be able to recover the three numerical functions of which I have spoken, and concerning which I have not found any indication in the papers left by the author. This would assuredly be a very interesting gap to fill.*

Later in 1913, Laisant [Bel24] updated his 1896 question through a response to a letter written by D. E. Smith at the behest of E. T. Bell. Bell wanted to know whether there was anything beyond what is asserted in the above-mentioned memoir concerning the connection between recurring series and elliptic functions.

> *The mathematical papers of Lucas, after his death, were entrusted to a commission of three members: M. Delannoy, Lemoine and myself. We found in them the necessary elements for the publication of the last two volumes (iii and iv) of the* Récréations Mathématiques, *and of the volume* Arithémique Amusant.
>
> *The remainder consisted of scattered notes which, in our estimation,*

were not available for publication .... I found no trace of the subject about which you particularly enquire, and I regret it keenly. I had studied with great interest the memoir Sur les fonctions numériques simplement périodiques, *and I often chatted over it with the author. These functions U, V, derived from the equation of the second degree present curious analogies with the sine and cosine. Lucas has also considered three functions derived from the equation of the third degree, on which he once made a communication to the Mathematical Society of France. I can find no trace of this communication, and I have lost all memory of it. I recall only the definition of one of these functions; it was $a^n + b^n + c^n$, a, b, c, being the roots of the equation. From the point of view of periodicity these functions exhibited the closest analogies with sn, cn, dn of elliptic functions. They presented certain characters of double periodicity.*

Lucas, in a conversation at his house, said to me: 'if we could prove that these functions admit only a single system of periods, Fermat's Theorem would be demonstrated.' And, making this assumption, he developed this proof for me in less than a quarter of an hour. Now I have completely lost all recollection of it. That was some months before his death, which I did not in the least anticipate. Since then I proposed a question on this subject in this Intermédiare. *It has remained unanswered .... I am more and more confirmed in my conviction that Lucas' premature death was an irreparable loss to the science of numbers....*

In response to a 1930 letter written by Duncan Harkin, Bell [Bel30] responded,

> *... you ask about a feasible generalization through elliptic functions of the Functions of Lucas. If I knew how to do this, I [s]hould be far from telling you, as I have tried my darndest to make some real progress on it myself for the past twentyeight [sic] years. It is a tough nut of the first order. Whoever cracks it will make a contribution to the theory of numbers on a par with anything Fermat did. Go to it!*

1.3 Commentary

On examining the material in the previous section, we note several properties of Lucas' 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 methods 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.

However, there was another aspect of this study: periodicity. As mentioned in Section 1.1, Lucas was very impressed by the close analogy between his functions

and the circular functions—functions that are singly periodic—and derived a kind of numerical periodicity for his functions. It is clear from what little he did write on this matter that he considered an attempt at generalizing his functions should begin by looking at doubly periodic functions, such as elliptic functions. It seems that Lucas believed (probably by analogy) that the numerical functions that would be derived through this analysis should exhibit the property of being doubly (numerically) periodic. However, it is not clear what this property would have been. Suppose we try the following definition of such a function.

Definition 1.1. *Let $H(x)$ be a function of an integer variable x such that $H(x)$ is also an integer. We will say that $H(x)$ is doubly numerically periodic modulo m, if there exists a pair of positive integers p_1 and p_2 such that $p_1 < p_2$, p_1 does not divide p_2 and p_1 is the least positive integer such that*

$$H(n+p_1) \equiv H(n) \pmod{m} \quad \textit{and} \quad H(n+p_2) \equiv H(n) \pmod{m}$$

for all sufficiently large values of n.

This seems to be the direct doubly periodic analog of a singly periodic numerical function like U_n or V_n, but no such function can exist. For suppose that for some m such a function $H(x)$ does exist. By the definition, we must have positive integers p_1 and p_2 such that

$$H(n + rp_1 + sp_2) \equiv H(n) \pmod{m}$$

for any fixed pair of integers r, s and all n sufficiently large. Suppose we specify r, s to be integers such that $rp_1 + sp_2 = d$, where $d = (p_1, p_2)$. Since p_1 does not

divide p_2, we must have $d < p_1$. However, for all sufficiently large n we must have $H(n+d) \equiv H(n) \pmod{m}$ with $0 < d < p_1$, a contradiction to the definition of p_1.

Thus, there are no doubly period numerical functions that would be similar to the Lucas functions. Nevertheless, Lucas' intuition that elliptic functions would be helpful was moving him in a very productive direction. Unfortunately, he did not possess the mathematical knowledge, nor did such knowledge exist until the 20^{th} century, to take advantage of his rather vague ideas. This is explained in some detail in Chapter 17 of [Wil98] and needs no further elaboration here. What is important to note is that his belief that linear recurring sequences would play a role in this approach led him to a dead end.

If, instead, we focus our attention on certain symmetric functions of the zeros α, β, γ of a cubic polynomial which also satisfy linear recurrences, we would certainly examine $S_n = \alpha^n + \beta^n + \gamma^n$, which is what Lucas did for the particular polynomial $x^3 - x - 1$. This particular sequence S'_n is now called the Perrin sequence, and was the focus of much attention by Adams and Shanks [AS82]. It seems first to have been considered by Catalan in 1861 (see Chapter 8 of [Déc99]). Catalan, who denoted the sequence by A_n, believed that A_n is or is not divisible by n according to whether or not n is a prime. This could easily be converted into a primality test that would execute in polynomial time in $\log n$, but unfortunately, Catalan's assertion is untrue. For example, we see in [AS82] that $271441 (= 521^2)$ divides A_{271441}; many other examples of this phenomenon are also provided. We should remark here that some of the work in [AS82] was later extended by Szekeres [Sze96]. Décaillot [Déc99] has raised the interesting possibility that Lucas was aware of Catalan's work before he (Lucas) embarked on his work in primality testing and that it might have inspired him

in his investigations. However, Lucas, who knew Catalan and who is usually most punctilious about assigning priority, nowhere mentions Catalan's work. Also, his result concerning this matter is more carefully stated than Catalan's, even though the proof is incomplete. Perhaps Lucas did not want to embarrass Catalan by mentioning his less circumspect work.

Laisant raised the intriguing possibility that Lucas was considering three functions that were symmetric functions of α, β, γ, one of which was S_n; what were the other two functions? In his attempt to interpret Lucas' 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 β and γ. Clearly, these functions are symmetric functions of α, β, γ. 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 Bell's x_n, y_n, 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. Nevertheless, the author's notes, certain passages of his correspondence, and the reprinting of some of his little known memoirs, would constitute an interesting volume for those interested in the higher arithmetic. This is a project which has not been completely abandoned, but whose realization will not be soon, whenever it does happen.*

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.

1.4 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 α, β, γ are the zeros of a cubic

polynomial $f(x)$, de Longchamps considered D_n, E_n and S_n, where

$$\begin{aligned} R^n D_n &= (\alpha^n + \beta^n)(\beta^n + \gamma^n)(\gamma^n + \alpha^n), \\ R^n E_n &= \frac{(\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)}{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)}, \\ S_n &= \alpha^n + \beta^n + \gamma^n, \end{aligned}$$

to be the degree three recurring function analogs of the Lucas functions. Are these the three functions that Laisant mentioned? 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 he (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, as we have seen in Section 1.2, Lucas had certainly mentioned 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.

The next work done on this problem was that of Pierce [Pie16] in 1916. He defined the two functions

$$S_m = \prod(1 + \alpha_i^m) \quad \text{and} \quad \Delta_m = \prod(1 - \alpha_i^m),$$

where the product is taken over all the zeros of a given polynomial $f(x)$ with integral coefficients. Pierce obtained several number theoretic results concerning these functions, particularly when the degree of $f(x)$ is three. Later, Lehmer [Leh33] extended some of Pierce's results, showing, among other things, that each satisfies a linear recurrence relation. Indeed, Lehmer [Leh71], [Leh68] made use of these functions in

a test, which makes use of the factors of $N^2 + N + 1$ to demonstrate the primality of N. Unfortunately, Pierce's functions are difficult to compute, which means that using them is not very practical. While Pierce's work represents a kind of extension of the Lucas functions, it is very unlikely that Lucas was thinking in this direction, because nowhere in his work does he allude to anything like these functions. Also, Pierce's functions do not become U_n and V_n when $f(x)$ is of degree two.

In 1929, Carmichael advocated to study the functions which he denoted by G_n and H_n. Although it appears that Carmichael was unaware of this, Lucas had mentioned both in his published work. The function G_n occurs as U_n on page 306 of [Luc91b] (also, in the cubic case G_n is the same as Bell's z_n) and H_n is the same as $\Delta(a^n, b^n, c^n, \dots)/\Delta(a, b, c, \dots)$. Carmichael stated that an investigation of the properties of these two functions would lead to two generalizations of Lucas' U_n function, but he did not follow up on this remark.

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], Engstrom [Eng31] and Ward [War31b], [War31c], [War33], [War36], [War37], [War55] investigated the arithmetical theory of linear recurring sequences, but they did not produce a set of functions which were analogous to Lucas' U_n and V_n. One of the most important properties of Lucas' function U_n is that it satisfies the condition of being a divisibility sequence; that is, the sequence

of integers $\{U_n\}$ $(n > 0)$ 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. Both Hall [Hal36] and Ward were interested in the problem of whether any function satisfying a linear recurrence could also be a divisibility sequence. While they did not succeed in answering this question completely (this was done later by Bézivin, Pethö and van der Poorten [BPvdP90]), they did show that this would be a very unlikely property for a sequence satisfying a third order recurrence unless it was a very uninteresting sequence, such as a special sequence satisfying $U_{n+3} = RU_n$. Indeed, one of the simplest, non-trivial, linear divisibility sequence after Lucas' U_n is $\Delta(\alpha^n, \beta^n, \gamma^n)/\Delta(\alpha, \beta, \gamma)$, where α, β, γ are the zeros of a cubic polynomial with integral coefficients. Ward, who was Bell's PhD student, seems to have contracted Bell's enthusiasm for extending Lucas' functions. In fact, he coined the term "lucasian" for any function satisfying a linear recurrence which was also a divisibility sequence. In [War38] he discussed two candidates for lucasian sequences, one of which we will discuss in great detail in this work. Of all the individuals who worked on the problem of extending the Lucas functions, he seems to have made the most progress. While we have mentioned only a few of his publications here, there are many more that are also of some relevance to this discussion and we urge the interested reader to consult the list of his published papers in [Leh93].

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. Although in the case where $f(x)$ is of degree three, it is

possible to use certain of these functions to extend (1.1) and (1.2), by making use of the tresine and cotresine functions of Graves [Gra47].

1.5 Our Objective

While many researchers have looked directly or peripherally at the problem of extending Lucas' 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 Longchamps' original suggestion.

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

$$\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha), \quad \Delta = \delta^2 = P^2Q^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2,$$

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

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

Note that C_n is the same as Lucas' $\Delta(\alpha^n, \beta^n, \gamma^n)/\Delta(\alpha, \beta, \gamma)(= R^nE_n)$ 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 α, β, γ 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 Chapter 2 we will list 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, and this seems to be the tenor of his remarks in Section 1.2 above. In the succeeding chapters 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.

The main tools that we will employ 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] above), 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 4.18. Lucas might have been aware of some of this material because he claims in part CLIX of [Luc80] that he was working, together with a 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 the proof might not have been completely rigorous. In the Appendix, we provide an alternate, more elementary proof of Theorem 4.18, which Lucas should 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].

Chapter 2

Lucas Sequences

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

$$U_n = U_n(P, Q) = (\alpha^n - \beta^n)/(\alpha - \beta), \tag{2.1}$$

$$V_n = V_n(P, Q) = \alpha^n + \beta^n, \tag{2.2}$$

where α and β 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, V_n satisfy the following equality

$$X_{n+2m} = V_m X_{n+m} - Q^m X_n, \tag{2.3}$$

where $U_0 = 0$, $U_1 = 1$, $V_0 = 2$ and $V_1 = P$.

Substituting $n - m$ for n in (2.3) gives both

$$U_{n+m} = V_m U_n - Q^m U_{n-m} \quad \text{and} \quad V_{n+m} = V_m V_n - Q^m V_{n-m}. \tag{2.4}$$

If the mth and nth terms are known, the $(m+n)$th term of a Lucas function may be found using the addition formulas presented below:

$$2U_{m+n} = V_m U_n + U_m V_n, \tag{2.5}$$

$$2V_{m+n} = V_m V_n + \Delta U_m U_n. \tag{2.6}$$

Now, if the facts $Q^n U_{-n} = -U_n$ and $Q^n V_{-n} = V_n$ are used in (2.5) and (2.6), the following subtraction formulas can be derived:

$$2Q^m U_{n-m} = U_n V_m - V_n U_m, \tag{2.7}$$

$$2Q^m V_{n-m} = V_n V_m - \Delta U_n U_m. \tag{2.8}$$

Subtracting (2.5) and (2.7) yields

$$U_{n+m} = V_n U_m + Q^m U_{n-m}. \tag{2.9}$$

Doing the same with (2.6) and (2.8) gives

$$V_{m+n} = \Delta U_n U_m + Q^m V_{n-m}. \tag{2.10}$$

Furthermore, by writing U_n, V_n, Δ in terms of α, β, it is clear that

$$V_n^2 - \Delta U_n^2 = 4Q^n \tag{2.11}$$

A doubling formula for U_n follows from (2.5) and a doubling formula for V_n follows from (2.6) and (2.11) to yield

$$U_{2n} = V_n U_n, \tag{2.12}$$

$$V_{2n} = V_n^2 - 2Q^n = \Delta U_n^2 + 2Q^n. \tag{2.13}$$

Of key importance to later sections, the following multiplication formulas for U_n and V_n can be obtained by use of the fact that $V_n + \delta U_n = 2\alpha^n$. From this we see that $2^{m-1}[V_{mn} + \delta U_{mn}] = [V_n + \delta U_n]^m$ and then expanding using the binomial theorem, we obtain

$$2^{m-1}U_{mn} = \sum_{i=0}^{\lfloor (m-1)/2 \rfloor} \binom{m}{2i+1} \Delta^i U_n^{2i+1} V_n^{m-2i-1}, \tag{2.14}$$

$$2^{m-1}V_{mn} = \sum_{i=0}^{\lfloor m/2 \rfloor} \binom{m}{2i} \Delta^i U_n^{2i} V_n^{m-2i}. \tag{2.15}$$

2.2 Computation of U_n, V_n

Often we are interested in calculating U_n or V_n, for some particular value of n. Although this can clearly be done via the formulas (2.1), (2.2) or equation (2.3), both methods are too slow for practical purposes. A faster method is presented here.

Let $(b_0 b_1 \dots b_k)_2$ be the binary representation of $m \in \mathbb{Z}^+$ such that $b_0 = 1$, $b_i \in \{0, 1\}$ for $(1 \leq i \leq k)$ and $k = \lfloor \log_2 m \rfloor$. The following formulas for Lucas sequences depend on identities (4.2.22) and (4.2.24) from [Wil98]:

$$\begin{aligned} U_{2n} &= 2U_{n+1}U_n - PU_n^2, \\ U_{2n+1} &= U_{n+1}^2 - QU_n^2, \\ U_{2n+2} &= PU_{n+1}^2 - 2QU_nU_{n+1}. \end{aligned}$$

Now, if $\mathcal{P}_0 = \{1, P\}$ and

$$\mathcal{P}_{i+1} = \begin{cases} \{2AB - PA^2, B^2 - QA^2\} & \text{if } b_{i+1} = 0, \\ \{B^2 - QA^2, PB^2 - 2QAB\} & \text{if } b_{i+1} = 1, \end{cases}$$

where $\mathcal{P}_i = \{A, B\}$, then $\mathcal{P}_k = \{U_m, U_{m+1}\}$. Moreover, one may use $\mathcal{P}_k$ to compute V_m, as

$$V_m = 2U_{m+1} - PU_m.$$

Hence U_m (V_m) can be computed in $O(\log m)$ multiplications and additions. Note that this result can be employed to compute U_m (V_m) (mod N) quickly by defining

$$\mathcal{P}_{i+1} = \begin{cases} \{2AB - PA^2, B^2 - QA^2\} \pmod N & \text{if } b_{i+1} = 0, \\ \{B^2 - QA^2, PB^2 - 2QAB\} \pmod N & \text{if } b_{i+1} = 1. \end{cases}$$

This is a more useful result as the growth of U_m is exponential.

Now let

$$W_n \equiv Q^{-n} V_{2n} \pmod N.$$

Then clearly

$$W_1 \equiv P^2 Q^{-1} - 2 \pmod N$$

and by (2.13)

$$W_{2n} \equiv W_n^2 - 2 \pmod N.$$

Further, by (2.4) replacing n by $2n + 2$ and m by $2n$, we have

$$V_{4n+2} = V_{2n} V_{2n+2} - Q^{2n} V_2;$$

so then

$$W_{2n+1} \equiv W_n W_{n+1} - W_1 \pmod N.$$

In this case define $\mathcal{P}_0 = \{W_1, W_2\}$ and

$$\mathcal{P}_{i+1} = \begin{cases} \{A^2 - 2, AB - W_1\} \pmod N & \text{if } b_{i+1} = 0, \\ \{AB - W_1, B^2 - 2\} \pmod N & \text{if } b_{i+1} = 1, \end{cases}$$

where $\mathcal{P}_i = \{A, B\}$, then

$$\mathcal{P}_k = \{W_m, W_{m+1}\}.$$

This method for finding $\{W_n, W_{n+1}\} \pmod N$ is faster to compute than the previous method for U_n or $V_n \pmod N$. Moreover, this method may also be used to find a particular value of U_n or $V_n \pmod N$ as follows. First,

$$V_{2h} \equiv Q^h W_h \pmod N,$$

and by (2.3) with $m = 1$ and $n = 2h + 1$ we have

$$PV_{2h+1} \equiv Q^{h+1}(W_{h+1} + W_h) \pmod N.$$

Also, by (2.10) with $m = 1$ and $n = 2h + 1$,

$$\Delta U_{2h+1} \equiv Q^{h+1}(W_{h+1} - W_h) \pmod N.$$

To complete this a formula for $U_{2h} \pmod N$ is needed in terms of W_h and W_{h+1}. This is achieved by the use of (2.6) with $m = 2h$ and $n = 2$ to see

$$2V_{2+2h} = (P^2 - 2Q)V_{2h} + \Delta P U_{2h},$$

and hence

$$\Delta P U_{2h} \equiv Q^h(2QW_{h+1} - (P^2 - 2Q)W_h) \pmod N.$$

2.3 Arithmetic Results

The identities from the previous section may be employed to construct arithmetic results for Lucas sequences. The global arithmetic results presented here are standard.

Definition 2.1. *If a and b are not both zero, then the* greatest common divisor (gcd) *of a and b is defined to be the largest integer that divides both a and b, denoted by (a, b).*

Definition 2.2. *If a and b are nonzero integers, then the* least common multiple (lcm) *of a and b is defined to be the least positive integer l such that $a \mid l$ and $b \mid l$, denoted by $[a, b]$.*

To begin, by the use of equation (2.11) it may be shown that

$$(U_n, V_n) \mid 2Q^n. \tag{2.16}$$

If $(P, Q) = 1$, then by setting $m = 1$ in equation (2.3) and by induction it is clear that for $n > 0$, we have

$$(U_n, Q) = (V_n, Q) = 1, \tag{2.17}$$

and hence for any $n \geq 0$

$$(U_n, V_n) \mid 2. \tag{2.18}$$

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

$$U_m \mid U_n, \quad \text{when} \quad m \mid n. \tag{2.19}$$

Note that if $n = ms$, then

$$\begin{aligned} U_n(P, Q) &= \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^{ms} - \beta^{ms}}{\alpha - \beta} \\ &= \frac{\alpha^m - \beta^m}{\alpha - \beta} \cdot \frac{\alpha^{ms} - \beta^{ms}}{\alpha^m - \beta^m} = U_m(P, Q) \cdot U_s(V_m, Q^m). \end{aligned}$$

Definition 2.3. *Given $m \in \mathbb{Z}$, let ω 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 $\omega(m)$.*

The next theorem is the first local theorem to be seen here. It does however have a global result as a corollary.

Theorem 2.4. *Let $(Q, m) = 1$ and $\omega = \omega(m)$. If $m \mid U_n$ for some $n > 0$, then $\omega \mid n$.*

Proof. Put

$$n = q\omega + r \text{ where } 0 \leq r < \omega.$$

If $r = 0$, then we are done. Thus we assume $r > 0$. Also,

$$n = (q+1)\omega - (\omega - r).$$

Since either q or $q+1$ is even, without loss of generality, let

$$n = q\omega + s \text{ where } 2 \mid q \quad \text{and} \quad |s| < \omega.$$

Setting $m = \frac{q\omega}{2} + s$ and $n = \frac{q\omega}{2}$ in (2.4) produces

$$U_n = U_{(\frac{q\omega}{2}+s)+\frac{q\omega}{2}} = U_{\frac{q\omega}{2}} V_{\frac{q\omega}{2}+s} - Q^{\frac{q\omega}{2}+s} U_{-s}.$$

Now since $m \mid U_n$ and $m \mid U_{\frac{q\omega}{2}} \Rightarrow m \mid Q^{\frac{q\omega}{2}+s} U_{-s}$. Note that s may be positive or negative. If $s > 0$, then $U_{-s} = Q^{-s} U_s \Rightarrow m \mid Q^{\frac{q\omega}{2}} U_s$. Hence $m \mid U_{|s|}$. But $|s| < \omega$, so by the minimality of ω, it must be that $s = 0 \Rightarrow \omega \mid n$.

□

Corollary 2.4.1. *If m, $n > 0$ and $d = (m, n)$, then*

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

Proof. Let $G = (U_m, U_n)$, then $U_d \mid G$, since $U_d \mid U_m$ and $U_d \mid U_n$. Let $\omega = \omega(G)$ be the rank of apparition of G. Then by Theorem 2.4 $\omega \mid m$ and $\omega \mid n \Rightarrow \omega \mid d \Rightarrow G \mid U_d$. Thus, $G = |U_d|$. □

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

Theorem 2.5. *If m, $n \geq 1$, then*

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

Proof. Let $r = \lfloor m/2 \rfloor$, then it may be shown that

$$(U_{mn}/U_n, U_n) \mid mQ^{nr}.$$

From the identity (4.2.41) of [Wil98]

$$U_{(2r+1)n} = U_n \sum_{j=0}^{r} \frac{2r+1}{r-j} \binom{r+j}{r-j-1} Q^{n(r-j)} \Delta^j U_n^{2j}$$

with $m = 2r + 1$, we get

$$U_{(2r+1)n}/U_n \equiv (2r+1)Q^{nr} \pmod{U_n}.$$

Thus, if $2 \nmid m$, then

$$(U_{mn}/U_n, U_n) \mid mQ^{nr}.$$

Also, from the identity (4.2.43) of [Wil98] we can write

$$U_{2rn} = V_n \sum_{j=0}^{r-1} \binom{r+j}{r-j-1} Q^{n(r-j-1)} \Delta^j U_n^{2j+1}.$$

So, if $m = 2r$, then

$$U_{2rn}/U_n \equiv rV_n Q^{n(r-1)} \pmod{U_n};$$

thus

$$(U_{2rn}/U_n, U_n) = (rV_nQ^{n(r-1)}, U_n).$$

Now

$$(rV_nQ^{n(r-1)}, U_n) \mid rQ^{n(r-1)}(V_n, U_n);$$

hence, it follows from (2.16) that

$$(U_{mn}/U_n, U_n) \mid mQ^{nr}$$

when $2 \mid m$. Lastly, since $(P, Q) = 1$, we have

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

from (2.17). □

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 2.6. *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 $p^{\lambda+1} \mid U_{pn}$.*

Proof. Let $p^\lambda \mid\mid U_n$ for some $\lambda \geq 1$. If $p = 2$, then by (2.11) $2 \mid V_n$, and since $U_{2n} = U_nV_n$, we get $2^{\lambda+1} \mid U_{2n}$.

Now if $\lambda > 1$, and $p = 2$, then Q is odd, hence by (2.11) $2 \mid\mid V_n$; thus in this case

$$2^{\lambda+1} \mid\mid U_{2n}.$$

If p is an odd prime, then by (2.14) with $m = p$, one has

$$2^{p-1}U_{pn} \equiv pU_n V_n^{p-1} \pmod{p^{\lambda+2}}.$$

Since $p \nmid Q$, then $p \nmid V_n$ by (2.11); thus

$$p^{\lambda+1} \mid\mid U_{pn}.$$

□

Definition 2.7. *Let $\epsilon(n)$ be the Jacobi symbol of (Δ/n).*

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

Theorem 2.8. *If p is a prime such that $p \nmid 2Q$, then $p \mid U_{p-\epsilon}$.*

Proof. First, note that $p \mid \binom{p}{i}$ for $i \neq 0, p$. So by (2.14) and (2.15), with $n = 1$ and $m = p$, the following congruences exist

$$2^{p-1}U_p \equiv \Delta^{\frac{p-1}{2}} \pmod{p}, \;\; 2^{p-1}V_p \equiv P^p \pmod{p}.$$

So by Fermat's little theorem and Euler's criterion for quadratic residuacity

$$U_p \equiv \epsilon \pmod{p}, \;\; V_p \equiv P \pmod{p}. \tag{2.20}$$

Thus if $\epsilon = 0$, then $p \mid U_{p-\epsilon}$. If $\epsilon \neq 0$, then we can use (2.5), (2.6), (2.7)and (2.8) to deduce

$$2Q^{\frac{1+\epsilon}{2}}U_{p-\epsilon} \equiv PU_p - \epsilon V_p \pmod{p}, \tag{2.21}$$

$$2Q^{\frac{1+\epsilon}{2}}V_{p-\epsilon} \equiv PV_p - \epsilon\Delta U_p \pmod{p}. \tag{2.22}$$

Thus by (2.20) $p \mid U_{p-\epsilon}$ when p is odd. □

In the sequel we will need the following result.

$$V_{p-\epsilon} \equiv 2Q^{\frac{1-\epsilon}{2}} \pmod{p}. \tag{2.23}$$

This follows easily from (2.22).

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. Observe the following short lemma that will be called upon in the next two theorems.

Lemma 2.9. *If* $2 \mid P$, *then* $2 \mid V_n$ *for all* $n \geq 0$. *If* $2 \nmid P$ *and* $2 \mid Q$, *then* $2 \mid V_n$ *only for* $n = 0$. *If* $2 \nmid P$ *and* $2 \nmid Q$, *then* $2 \mid V_n \Leftrightarrow 3 \mid n$.

Proof. Certainly, if $2 \mid P$, then $2 \mid V_k$ for all $k \geq 0$. If $2 \nmid P$, then since $V_1 = P$ and $V_{k+1} \equiv PV_k \pmod{Q}$, we see that if $2 \mid Q$, then $2 \nmid V_n$ for $n > 0$. If $2 \nmid P$ and $2 \nmid Q$, it follows by using induction on (2.3) that $2 \mid V_k$ if and only if $3 \mid k$. □

Note that from the above lemma we can easily see that if $2 \mid V_n$, then $2 \mid V_{tn}$ for all $t \in \mathbb{N}$. 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 2.10. *If* $m \mid n$ *and* $2 \nmid \frac{n}{m}$, *then* $V_m \mid V_n$.

Proof. Since $m \mid n$ and $2 \nmid \frac{n}{m}$, then $n = km$ where k odd, i.e. $k = 2r + 1$ for some $r \in \mathbb{Z}$. From (2.6)

$$2V_n = 2V_{km} = 2V_{(2r+1)m} = 2V_{2rm+m} = V_m V_{2rm} + \Delta U_m U_{2rm}.$$

Since $V_m^2 - \Delta U_m^2 = 4Q^m$, if $2 \mid V_m$, then $2 \mid \Delta U_m$. Also, $V_m \mid U_{2m}$ and $U_{2m} \mid U_{2rm}$ implies $V_m \mid U_{2rm}$, hence, $V_m \mid 2V_{km}$. If $2 \mid V_m$, then by Lemma 2.9, $2V_m \mid 2V_{km} \Rightarrow V_m \mid V_{km}$. On the other hand, if $2 \nmid V_m$, then $V_m \mid V_{km}$. □

Note that if $r \mid V_n$ and $n > 0$, then since $(V_n, Q) = 1$, it must be that $(r, Q) = 1$. Also, since $V_{-n} = V_n/Q^n$, we may write $r \mid V_{-n}$. This simply means that r divides the integral numerator of the fraction V_{-n}.

Theorem 2.11. *If $m \mid n$ and $2 \mid \frac{n}{m}$, then $(V_m, V_n) \mid 2$.*

Proof. We first employ (2.13) and (2.17) to observe that

$$V_{2m} = V_m^2 - 2Q^m \Rightarrow (V_m, V_{2m}) = (2Q^m, V_m) = (2, V_m).$$

Hence $(V_m, V_{2m}) \mid 2$. Now assume $(V_m, V_{2km}) \mid 2$, this is certainly true for $k = 1$, then since

$$V_{(2k+2)m} = V_m V_{(2k+1)m} - Q^m V_{2km},$$

we find that $(V_{(2k+2)m}, V_m) = (Q^m V_{2km}, V_m) = (V_{2km}, V_m)$. Thus the result follows by induction.

□

Corollary 2.11.1. *If $2 \mid m$, then $(V_n, V_{mn}) = (2, V_n)$.*

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 2.12. *Suppose $r \mid V_n$ $(n > 0)$. Denote by $\rho(r)$ the least positive integer ρ such that $r \mid V_\rho$.*

In order to say something about $\rho(r)$ for $r \mid V_n$, the result below is needed first.

Lemma 2.13. *If $r \mid V_n$ and $r \mid V_m$, then $r \mid V_{2^k m+n}$ $(k \geq 1)$.*

Proof. By (2.6) we have

$$2V_{2^k m+n} = V_{2^k m}V_n + \Delta U_{2^k m}U_n.$$

Now $r \mid V_m \Rightarrow r \mid U_{2m}$ by (2.12). Consequently, $r \mid U_{2^k m}$ for any integral $k \geq 1$. Thus, since $r \mid V_n$ and $r \mid U_{2^k m}$ we have $r|2V_{2^k m+n}$. If $2 \nmid r$, the desired result is obtained. On the other hand, if $2 \mid r$, then $2 \mid V_m$, and by Lemma 2.9, $2 \mid V_{2^k m}$. Also, $2 \mid V_n$ and $2 \mid \Delta U_n$, as $V_n^2 + \Delta U_n^2 = 4Q^n$. Hence $2r \mid 2V_{2^k m+n} \Rightarrow r \mid V_{2^k m+n}$. □

The theorem below is a local arithmetic result for $\{V_n\}$ and is very similar to Theorem 2.4 as seen for $\{U_n\}$, though the method of proof is different.

Theorem 2.14. *If $r \mid V_n$ $(n > 0)$, then $\rho(r) \mid n$.*

Proof. Let $2^\mu \mid\mid (n, \rho)$. Then $2^\mu \mid\mid n$ or $2^\mu \mid\mid \rho$. Suppose, $2^\mu \mid\mid n$, then $2^\mu \mid\mid d$, where $d = (2\rho, n)$. There exist $x, y \in \mathbb{Z}$ such that

$$d = 2\rho x + ny \Rightarrow \frac{d}{2^\mu} = \frac{2\rho x}{2^\mu} + \frac{ny}{2^\mu}.$$

Now, $2 \mid \frac{2\rho}{2^\mu}$ and $2 \nmid \frac{d}{2^\mu} \Rightarrow 2 \nmid y$ so by Theorem 2.10 $r \mid V_{yn}$. Let $2^k \mid\mid 2x$, then $V_d = V_{2^k \frac{2x}{2^k}\rho+yn}$, and since $r \mid V_\rho$ again, by Theorem 2.10 $r \mid V_{\frac{2x}{2^k}\rho}$ because $2 \nmid 2x/2^k$. Thus, $r \mid V_d$ by the previous lemma. Hence, $d \geq \rho$. But $d \mid 2\rho \Rightarrow \frac{d}{2^\mu} \mid \frac{2\rho}{2^\mu}$ and since $\frac{d}{2^\mu}$ is odd, we get $\frac{d}{2^\mu} \mid \frac{\rho}{2^\mu}$ which means that $d \mid \rho \Rightarrow d = \rho$. Since $d \mid n$, we have completed the proof for this case.

Next suppose that $2^\mu \mid\mid \rho$ and $2^{\mu+1} \mid n$. Put $d = (\rho, 2n) \Rightarrow 2^\mu \mid\mid d$. There exist $x, y \in \mathbb{Z}$ such that

$$d = \rho x + 2ny \Rightarrow \frac{d}{2^\mu} = \frac{\rho x}{2^\mu} + \frac{2ny}{2^\mu}.$$

Here, $2 \nmid \frac{d}{2^\mu}$ and $2 \mid \frac{2n}{2^\mu} \Rightarrow 2 \nmid x \Rightarrow r \mid V_{x\rho}$. Let $2^k \mid\mid 2y$ $(y \geq 1)$. So, $V_d = V_{2^k \frac{2ny}{2^k} + x\rho}$, and since $r \mid V_{\frac{2y}{2^k} n}$ we get $r \mid V_d$ by the previous lemma. This implies $d \geq \rho$. But $d \mid \rho \Rightarrow d = \rho$. Also, as $d \mid 2n$ we must have $\rho \mid 2n$, which means that $\frac{\rho}{2^\mu} \mid \frac{2n}{2^\mu}$. Since $2 \nmid \frac{\rho}{2^\mu}$, then $\frac{\rho}{2^\mu} \mid \frac{n}{2^\mu} \Rightarrow \rho \mid n$. □

A consequence of Corollary 2.11.1 is the following helpful result which will be called upon in three of the next four theorems.

Lemma 2.15. *If $r > 2$ and $r \mid V_n$, then $2 \nmid \frac{n}{\rho(r)}$.*

Proof. Suppose $2 \mid \frac{n}{\rho(r)}$, then $n = m\rho$, where m is even. Thus, by Corollary 2.11.1

$$(V_\rho, V_n) = (V_\rho, V_{m\rho}) = (2, V_\rho) \leq 2.$$

This is a contradiction since $r \mid (V_\rho, V_n)$ and $r > 2$. □

The next two theorems cover what can be said about $r_1 r_2 \mid V_s$ for some s, when we know that $r_1 \mid V_n$ and $r_2 \mid V_m$. The results here really depend on how many factors of 2 the quantities m and n have and hence there are two cases: the first case, $2^\mu \mid\mid n$ and $2^\mu \mid\mid m$, is addressed in Theorem 2.16 and the second case, $2^\mu \mid\mid n$ and $2^\nu \mid\mid n$ $(\mu \neq \nu)$, in Theorem 2.17.

Theorem 2.16. *If $r_1 \mid V_m$, $r_2 \mid V_n$, $(r_1, r_2) = 1$, $2^\mu \mid\mid m$ and $2^\mu \mid\mid n$, then*

$$r_1 r_2 \mid V_{[m,n]}.$$

Proof. Note, $\frac{[m,n]}{m}$ and $\frac{[m,n]}{n}$ are both odd. It follows from Theorem 2.10 that

$$r_1 \mid V_{m\frac{[m,n]}{m}} \quad \text{and} \quad r_2 \mid V_{n\frac{[m,n]}{n}}.$$

Since $(r_1, r_2) = 1$, $r_1 r_2 \mid V_{[m,n]}$. □

Theorem 2.17. *If $r_1 \mid V_m$, $r_2 \mid V_n$, $(r_1, r_2) = 1$, $r_1, r_2 > 2$, $2^\mu \mid\mid m$ and $2^\nu \mid\mid n$ $(\mu \neq \nu)$, then $r_1 r_2 \nmid V_k$ for every $k \in \mathbb{Z}$.*

Proof. Let $\rho_1 = \rho(r_1)$ and $\rho_2 = \rho(r_2)$. Since, $r_1, r_2 > 2$, by Theorem 2.14 and Lemma 2.15,

$$\rho_1 \mid m, \quad \rho_2 \mid n \quad \text{and} \quad 2 \nmid \frac{m}{\rho_1}, \quad 2 \nmid \frac{n}{\rho_2}.$$

Thus, $2^\mu \mid\mid \rho_1$, $2^\nu \mid\mid \rho_2$. If $r_1 r_2 \mid V_s$, then $2 \nmid \frac{s}{\rho_1}$ and $2 \nmid \frac{s}{\rho_2} \Rightarrow 2^\mu \mid\mid s$ and $2^\nu \mid\mid s$. This is obviously a contradiction, so the wanted result is obtained. □

It has been established that for m, $n > 0$, $(U_m, U_n) = |U_{(m,n)}|$. A similar, but more complicated result exists for (V_m, V_n) and again it is dependent on the number of factors of 2 for m and n. The two cases are covered in the next two theorems.

Theorem 2.18. *If $2^\mu \mid\mid m$ and $2^\mu \mid\mid n$, then*

$$(V_m, V_n) = |V_{(m,n)}|.$$

Proof. Since $2^\mu \mid\mid m$ and $2^\mu \mid\mid n$, then $2 \nmid \frac{m}{(m,n)}$, $2 \nmid \frac{n}{(m,n)} \Rightarrow V_{(m,n)} \mid V_m$, $V_{(m,n)} \mid V_n$ by Theorem 2.10. Put $d = (V_m, V_n)$, then $V_{(m,n)} \mid d$.

Now note that $\rho(d) \mid m$, $\rho(d) \mid n \Rightarrow \rho(d) \mid (m, n)$. By Lemma 2.15, for $d > 2$, it must be that $2 \nmid \frac{m}{\rho(d)}$, $2 \nmid \frac{n}{\rho(d)} \Rightarrow 2 \nmid \frac{(m,n)}{\rho(d)}$. So then, by Theorem 2.10, $d \mid V_{(m,n)} \Rightarrow (V_m, V_n) = |V_{(m,n)}|$.

If $d = 1$, then we are done. If $d = 2$, then $2 \mid V_n$ and $2 \mid V_m$ so that, by Lemma 2.9, either $2 \mid P$ and $2 \mid V_{(m,n)}$, or $2 \nmid P$ and $3 \mid (m, n)$. Thus $2 \mid V_{(m,n)}$. □

Theorem 2.19. *If* $2^\mu \mid\mid m$ *and* $2^\nu \mid\mid n$ $(\mu \neq \nu)$*, then* $(V_m, V_n) \mid 2$*.*

Proof. Let $d = (V_m, V_n)$, then for $d > 2$, by Lemma 2.15 one must have $2 \nmid \frac{m}{\rho(d)}$, $2 \nmid \frac{n}{\rho(d)} \Rightarrow 2^\lambda \mid\mid m$, $2^\lambda \mid\mid n$, when $2^\lambda \mid\mid \rho(d)$. This is clearly a contradiction, thus $(V_m, V_n) \mid 2$, if $\mu \neq \nu$.

□

The short theorem below, which was known to Lucas, is of interest because it provides some insight into the characteristics of an odd prime p, when $p \mid V_n$.

Theorem 2.20. *If* p *is an odd prime and* $p \mid V_n$*, then* $p \equiv \pm 1 \pmod{2^{\nu+1}}$ *where* $2^\nu \mid\mid n$*.*

Proof. If $p \mid V_n$, then $p \nmid Q$ by (2.17). Also, by (2.11), we see that $p \nmid \Delta$ and $p \nmid U_n$. However, we do have $p \mid U_{2n}$ by (2.12). Thus, if ω is the rank of apparition of p, then $\omega \mid 2n$ by Theorem 2.4 and $\omega \nmid n$. Also, $\omega \mid p \pm 1$ by Theorem 2.8. So if $2^\nu \mid\mid n$, then $2^{\nu+1} \mid \omega \Rightarrow p \equiv \pm 1 \pmod{2^{\nu+1}}$. □

We have shown, in Theorem 2.8, 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 2.21. *If p is a prime such that $p \nmid 2\Delta Q$, then*

$$p \mid U_{\frac{p-\epsilon}{2}} \Leftrightarrow (Q/p) = 1,$$
$$p \mid V_{\frac{p-\epsilon}{2}} \Leftrightarrow (Q/p) = -1.$$

Proof. Setting $n = p - \epsilon$ in (2.13) yields

$$V_{p-\epsilon} = V^2_{\frac{p-\epsilon}{2}} - 2Q^{\frac{p-\epsilon}{2}}.$$

So then by (2.23),

$$V^2_{\frac{p-\epsilon}{2}} \equiv 2Q^{\frac{1-\epsilon}{2}} + 2Q^{\frac{p-\epsilon}{2}} \equiv 2Q^{\frac{1-\epsilon}{2}} + 2Q^{\frac{1-\epsilon}{2}}Q^{\frac{p-1}{2}} \equiv 2Q^{\frac{1-\epsilon}{2}}(1 + (Q/p)) \pmod{p}.$$

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

2.4 Primality Testing

Lucas' 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 2.22. *Suppose N is an odd integer. Let $T = T(N) = N + 1$ or $N - 1$. 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 2.23. *Suppose N is an odd integer. Let $T = T(N) = N + 1$ or $N - 1$. 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 2.23.1. *Suppose N is an odd integer and $T = T(N) = N + 1$ or $N - 1$. 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.*

Proof. By Theorem 2.5, we have

$$(U_T/U_{T/q}, U_{T/q}) \mid q.$$

Thus if $N \mid U_T/U_{T/q}$, then $N \nmid U_{T/q}$. The result follows by the theorem. □

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 2.24. *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*

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

Proof. Suppose $N \mid V_{\frac{N+1}{2}}(P, Q)$. Let p be some prime such that $p \mid N$, then $p \equiv \pm 1 \pmod{2^n}$ by Theorem 2.20. So $p = k2^n \pm 1$ for some $k \in \mathbb{Z}$. Assume N is composite, then without loss of generality $N = pq$, where $p = k2^n + 1$, $q = l2^n - 1$ and l, $k > 0$. Thus

$$A2^n - 1 = N = pq = (k2^n + 1)(l2^n - 1) = (kl2^n + l - k)2^n - 1;$$

in particular

$$A = kl2^n - k + l.$$

Now if $l \geq k$, then $(kl2^n - k + l) \geq 2^n \Rightarrow A \geq 2^n$, which is a contradiction as $A < 2^n$. On the other hand, if $l < k$, then $l + 1 \leq k$ and since $l2^n - 1 > 0$ we have

$$\begin{aligned} kl2^n - k + l &= k(l2^n - 1) + l \geq (l+1)(l2^n - 1) + 1 \\ &= (l^2 + l)2^n - l \geq 2^{n+1} - 1 \geq 2^n. \end{aligned}$$

Again, this is a contradiction as $A < 2^n$. So N is a prime.

Now suppose N is a prime. Since $(\Delta/N) = -1$, then

$$U_{N+1} \equiv 0 \pmod{N}$$

by the law of apparition Theorem 2.8. Further, since $(Q/N) = -1$ we have

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

by Euler's criterion in Theorem 2.21. □

Corollary 2.24.1. *Suppose $A = 1$ and $2 \nmid n$, $n \geq 3$. Put $Q = -2$, $P \equiv 2 \pmod{N}$. Then N is a prime if and only if*

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

Proof. Since $\Delta \equiv 12 \pmod{N}$, we have $(\Delta/N) = (Q/N) = -1$. □

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

$$N \mid V_{\frac{N+1}{2}}(2, -2) \Leftrightarrow N | S_{n-2},$$

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 $N \mid S_{n-2}$. It is this corollary that provides an efficient test for Mersenne primes; for further information see [Leh35]. In fact, the largest prime ever found by hand calculation[1], $M_{127} = 2^{127} - 1$, was found by Lucas in 1876 using a result similar to this corollary. This was most remarkable as M_{127} is a 39 digit number. Strangely Lucas seems to have lacked confidence in this result, despite the robustness of a positive outcome. It is believed that Lucas only performed this test once as it has been estimated that he spent between 170 and 300 hours performing the necessary calculations. The world's largest known primes are still of the Mersenne form and continue to be found by use of the Lucas-Lehmer test via the GIMPS project (the great internet Mersenne prime search) [gim]. There are only 46 Mersenne primes known to date, the largest being $M_{43112609}$ which is an impressive 12978189 decimal digit number. For large primes of other forms we direct the reader to the website *the prime pages* maintained by Boris Iskra [Isk].

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

Theorem 2.25. *Let p be a prime such that $p \equiv -1 \pmod 4$. There exist P, Q such that $(\frac{\Delta}{p}) = (\frac{Q}{p}) = -1$ if and only if $Q \equiv \mathrm{N}(\lambda)$, $P \equiv \mathrm{Tr}(\lambda) \pmod p$, where $\lambda \in \mathbb{Z}[i]$ and $(\frac{\mathrm{N}(\lambda)}{p}) = -1$.*

Proof. Suppose $Q \equiv \mathrm{N}(\lambda)$, $P \equiv \mathrm{Tr}(\lambda) \pmod p$ and $(\frac{\mathrm{N}(\lambda)}{p}) = -1$. Then $(\frac{Q}{p}) =$

[1]Lucas did not actually write out the calculations but made a game of it, for details see [WS94]

$(\frac{\mathrm{N}(\lambda)}{p}) = -1$ and $\Delta = P^2 - 4Q = \mathrm{Tr}(\lambda)^2 - 4\,\mathrm{N}(\lambda)$. If $\lambda = a + bi$, then $\mathrm{Tr}(\lambda) = 2a$ and $\mathrm{N}(\lambda) = a^2 + b^2$, hence $\mathrm{Tr}(\lambda)^2 - 4\,\mathrm{N}(\lambda) = -4b^2$ and $(\frac{\Delta}{p}) = (\frac{-4b^2}{p}) = (\frac{-1}{p}) = -1$.

Now, suppose $(\frac{\Delta}{p}) = (\frac{Q}{p}) = -1$. We have $(\frac{P^2-4Q}{p}) = -1$, thus $(\frac{4Q-P^2}{p}) = 1$. Hence, there exists some $c \pmod p$ such that $4Q - P^2 \equiv c^2 \pmod p$ and hence $Q \equiv (2^{-1}P)^2 + (2^{-1}c)^2 \pmod p$. Putting $\lambda = a + bi$, where $a \equiv 2^{-1}P$, $b \equiv 2^{-1}c \pmod p$, we get $\lambda \in \mathbb{Z}[i]$, $P \equiv \mathrm{Tr}(\lambda)$, $Q \equiv \mathrm{N}(\lambda) \pmod p$ and $(\frac{\mathrm{N}(\lambda)}{p}) = -1$. $\square$

Chapter 3

A New Attempt to Generalize the Lucas Sequences

3.1 De Longchamps' Method

Perhaps the oldest cubic generalization of Lucas sequences was provided by Gastone Gohierre de Longchamps. If we let α, β, γ be the zeros of $X^3 - PX^2 + QX - R$, where P, Q, R are integers, then we can define the following sequences suggested by de Longchamps (1880)[dL80],

$$R^n D_n = (\alpha^n + \beta^n)(\beta^n + \gamma^n)(\gamma^n + \alpha^n),$$
$$R^n E_n = (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)/[(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)],$$
$$S_n = \alpha^n + \beta^n + \gamma^n,$$

Notice that if we let $\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$, then $\delta^2 = \Delta = Q^2P^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2$, where Δ is the discriminant of the above mentioned cubic. Also note that $\alpha + \beta + \gamma = P$, $\alpha\beta + \beta\gamma + \gamma\alpha = Q$ and $\alpha\beta\gamma = R$.

For the sake of clarity let us denote $R^n D_n = L_n$, $R^n E_n = C_n$ and $S_n = A_n$, so this notation will match the other generalizations. De Longchamps' work yielded a few interesting results, including the multiplicative formula

$$C_{2n} = L_n C_n.$$

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 σ_n nor τ_n are integer sequences.

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

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

Also,

$$\begin{aligned} S_nT_n &= R^nA_n^3 + B_n^3 - 6R^nA_nB_n + 9R^{2n} \\ &= R^nA_{3n} + B_{3n} + 3R^{2n} \quad \text{(see Theorem 3.5)}, \end{aligned}$$

where B_n is defined in the next section.

3.2 Another Cubic Generalization

In an attempt to develop a theory analogous to that of Lucas functions the following method was proposed by Williams (1998) [Wil98]. Again, there are three sequences defined in this generalization. As in the last method, let α, β, γ be the zeros of $X^3 - PX^2 + QX - R$, where P, Q, R are integers. Now define

$$A_n = \alpha^n + \beta^n + \gamma^n, \tag{3.1}$$

$$B_n = \alpha^n\beta^n + \beta^n\gamma^n + \gamma^n\alpha^n, \tag{3.2}$$

$$C_n = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\frac{\beta^n - \gamma^n}{\beta - \gamma}\right)\left(\frac{\gamma^n - \alpha^n}{\gamma - \alpha}\right). \tag{3.3}$$

Rather than a second order linear recurrence as in Theorem 2.3 for the Lucas case, there is the following result for A_n and B_n.

Theorem 3.1. *The sequences A_n and B_n respectively satisfy the following third order recurrence formulas,*

$$t_{n+3} = Pt_{n+2} - Qt_{n+1} + Rt_n,$$
$$t_{n+3} = Qt_{n+2} - RPt_{n+1} + R^2t_n.$$

Proof. First let

$$t_n = c_1\alpha^n + c_2\beta^n + c_3\gamma^n,$$

where c_i are constants. Then

$$\begin{aligned} t_{n+3} &= c_1\alpha^{n+3} + c_2\beta^{n+3} + c_3\gamma^{n+3} \\ &= c_1\alpha^n\alpha^3 + c_2\beta^n\beta^3 + c_3\gamma^n\gamma^3. \end{aligned}$$

Using the fact that α, β and γ are the roots of the polynomial $X^3 - PX^2 + QX - R$, we can observe

$$\begin{aligned} \alpha^3 &= P\alpha^2 - Q\alpha + R \\ \beta^3 &= P\beta^2 - Q\beta + R \\ \gamma^3 &= P\gamma^2 - Q\gamma + R. \end{aligned}$$

Substituting these equalities into our original equation for t_{n+3} gives

$$\begin{aligned} t_{n+3} &= c_1\alpha^n(P\alpha^2 - Q\alpha + R) + c_2\beta^n(P\beta^2 - Q\beta + R) \\ &+ c_3\gamma^n(P\gamma^2 - Q\gamma + R) \\ &= P(c_1\alpha^{n+2} + c_2\beta^{n+2} + c_3\gamma^{n+2}) - Q(c_1\alpha^{n+1} + c_2\beta^{n+1} + c_3\gamma^{n+1}) \\ &+ R(c_1\alpha^n + c_2\beta^n + c_3\gamma^n) \\ &= Pt_{n+2} - Qt_{n+1} + Rt_n. \end{aligned}$$

The recurrence relation for B_n follows from substituting $\alpha\beta$ for α, $\beta\gamma$ for β and $\gamma\alpha$ for γ in the above argument. □

The recurrence relation for C_n is not as simple as that for A_n and B_n and will be covered in a later section.

Some easily verified identities for generalized Lucas functions follow in the theorems below. The next result is a nice generalization of the facts $U_n = -Q^nU_{-n}$ and $V_n = Q^nV_{-n}$.

Theorem 3.2.

$$\begin{aligned} A_n &= R^nB_{-n}, \\ B_n &= R^nA_{-n} \ \ \textit{and} \\ C_n &= -R^{2n}C_{-n}. \end{aligned}$$

Proof.

$$\begin{aligned} R^nB_{-n} &= \alpha^n\beta^n\gamma^n\left(\alpha^{-n}\beta^{-n} + \beta^{-n}\gamma^{-n} + \gamma^{-n}\alpha^{-n}\right) \\ &= \gamma^n + \alpha^n + \beta^n = A_n. \end{aligned}$$

The proof for B_n and C_n follow by the same method, that is, writing both sides of the equation in terms of α, β and γ. □

If we write (2.11) as $\Delta U_n^2 = V_n^2 - 4Q^n$, then the following theorem is a useful generalization for this cubic case.

Theorem 3.3.

$$\Delta C_n^2 = A_n^2 B_n^2 + 18 A_n B_n R^n - 4B_n^3 - 4A_n^3 R^n - 27R^{2n},$$
$$27\Delta C_n^2 = 4(A_n^2 - 3B_n)^3 - (27R^n + 2A_n^3 - 9A_n B_n)^2.$$

There are also doubling formulas analogous to (2.12) and (2.13) and tripling formulas.

Theorem 3.4.

$$A_{2n} = A_n^2 - 2B_n,$$
$$B_{2n} = B_n^2 - 2R^n A_n,$$
$$C_{2n} = C_n(A_n B_n - R^n).$$

Theorem 3.5.

$$A_{3n} = A_n^3 - 3A_n B_n + 3R^n,$$
$$B_{3n} = B_n^3 - 3R^n A_n B_n + 3R^{2n},$$
$$C_{3n} = C_n(A_n^2 B_n^2 - B_n^3 - R^n A_n^3).$$

More general than the doubling or tripling formulas, there is the following theorem that provides some addition formulas for A_n and B_n.

Theorem 3.6.

$$A_{n+m} = A_n A_m - (B_n A_{m-n} - R^n A_{m-2n})$$

$$B_{n+m} = B_n B_m - R^n (A_n B_{m-n} - R^n B_{m-2n}).$$

Proof.

$$\begin{aligned}
A_n A_m &- (B_n A_{m-n} - R^n A_{m-2n}) = (\alpha^n + \beta^n + \gamma^n)(\alpha^m + \beta^m + \gamma^m) \\
&- [(\alpha^n\beta^n + \beta^n\gamma^n + \gamma^n\alpha^n)(\alpha^{m-n} + \beta^{m-n} + \gamma^{m-n}) \\
&- \alpha^n\beta^n\gamma^n(\alpha^{m-2n} + \beta^{m-2n} + \gamma^{m-2n})] \\
&= [\alpha^{n+m} + \beta^{n+m} + \gamma^{n+m} + \alpha^m\beta^n + \gamma^n\alpha^m + \alpha^n\beta^m + \gamma^n\beta^m + \alpha^n\gamma^m + \beta^n\gamma^m] \\
&- [(\alpha^m\beta^n + \alpha^{m-n}\beta^n\gamma^n + \gamma^n\alpha^m + \alpha^n\beta^m + \beta^m\gamma^n + \gamma^n\alpha^n\beta^{m-n} \\
&+ \gamma^{m-n}\alpha^n\beta^n + \beta^n\gamma^m + \gamma^m\alpha^n) - (\alpha^{m-n}\beta^n\gamma^n + \gamma^n\alpha^n\beta^{m-n} + \gamma^{m-n}\alpha^n\beta^n)] \\
&= \alpha^{n+m} + \beta^{n+m} + \gamma^{n+m} = A_{n+m}.
\end{aligned}$$

Similar methods are used to show $B_{n+m} = B_n B_m - R^n(A_n B_{m-n} - R^n B_{m-2n})$. □

Corollary 3.6.1.

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

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

Proof. These identities follow from the previous theorem by setting $R = 1$ and replacing α by α/β, β by β/γ and γ by γ/α. □

Note that historically Corollary 3.6.1 was discovered by de Longchamps in his original paper [dL80].

The addition identities together with the doubling and tripling formulas may then be used to derive the following results.

Theorem 3.7.

$$A_{5n} = A_n^5 - 5A_n^3 B_n + 5A_n^2 R^n + 5A_n B_n^2 - 5B_n R^n$$
$$B_{5n} = B_n^5 - 5B_n^3 A_n R^n + 5B_n^2 R^{2n} + 5B_n A_n^2 R^{2n} - 5A_n R^{3n}.$$

Proof. Replace the identities A_{2n}, B_{2n} and A_{3n} from Theorem 3.5 into the addition formula for A_{n+m} from Theorem 3.6 while setting $m = 4n$. Similarly use identities B_{2n}, A_{2n}, and B_{3n} from Theorem 3.5 into the addition formula for B_{n+m} from Theorem 3.6 setting $m = 4n$. □

Corollary 3.7.1.

$$\sigma_{5n} = \sigma_n^5 - 5\sigma_n^3 \tau_n + 5\sigma_n \tau_n^2 + 5\sigma_n^2 - 5\tau_n$$
$$\tau_{5n} = \tau_n^5 - 5\tau_n^3 \sigma_n + 5\tau_n \sigma_n^2 + 5\tau_n^2 - 5\sigma_n.$$

Proof. These identities follow from the previous theorem by setting $R = 1$ and replacing α by α/β, β by β/γ and γ by γ/α. □

3.3 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

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

where V is a *Vandermonde matrix*. Then we can define generalized Lucas sequences of degree m as follows:

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

Or, using the Leibniz formula,

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

and we define W_n by

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

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

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 $W_n = V_n$. Note that this

generalization only relies on the use of two sequences as in the original case, not the expected three as for the cubic case.

In an effort to achieve simplicity and clarity with the new generalization, we will restrict ourselves to the case where $m = 3$. As usual, let α, β, γ be the same as in the previous generalizations where P, Q and R are their elementary symmetric functions. We can put

$$\delta C_n = \left(\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}\right) - \left(\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n\right)$$

and

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

Theorem 3.8. *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

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

The proof of the above theorem follows on noting that both C_n and W_n are linear combinations of $\alpha^m\beta^{2m}$, $\beta^m\gamma^{2m}$, $\gamma^m\alpha^{2m}$, $\alpha^{2m}\beta^m$, $\beta^{2m}\gamma^m$, $\gamma^{2m}\alpha^m$ and these 6 quantities are the zeros of

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

Returning to de Longchamps' work, we can make the following observations. Letting $S_n = \alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}$, $T_n = \alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n$ as before, we have

$$\delta C_n = S_n - T_n, \quad W_n = S_n + T_n,$$

$$L_n = S_n + T_n + 2R^n \quad \text{and} \quad W_n = L_n - 2R^n = A_nB_n - 3R^n.$$

It is also true that

$$S_n = R^n\sigma_n \quad \text{and} \quad T_n = R^n\tau_n.$$

The relations above combine to yield the important formulas

$$S_n = R^n\sigma_n = \frac{W_n + \delta C_n}{2} \quad \text{and} \quad T_n = R^n\tau_n = \frac{W_n - \delta C_n}{2}. \tag{3.4}$$

One can easily verify that

$$\frac{W_n^2 - \Delta C_n^2}{4} \in \mathbb{Z}$$

by noting

$$\frac{W_n^2 - \Delta C_n^2}{4} = S_nT_n = 3R^{2n} + R^nA_{3n} + B_{3n} \tag{3.5}$$

$$= R^nA_n^3 + B_n^3 - 6R^nA_nB_n + 9R^{2n} \in \mathbb{Z}. \tag{3.6}$$

Theorem 3.9.

$$R^{2n}C_{-n} = -C_n \quad \textit{and} \quad R^{2n}W_{-n} = W_n.$$

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.

3.4 Addition Formulas for W_n and C_n

As in the historic generalizations for Lucas sequences, there exist addition formulas for C_n and W_n. These formulas build on de Longchamps' work, and are analogues of (2.5) and (2.6).

Theorem 3.10.

$$2W_{2n+m} = W_nW_{n+m} + \Delta C_nC_{n+m} - R^n(W_nW_m - \Delta C_nC_m - 2R^{2m}W_{n-m})$$
$$2C_{2n+m} = C_{n+m}W_n + C_nW_{n+m} - R^n(C_mW_n - C_nW_m + 2R^{2m}C_{n-m}).$$

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

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

Corollary 3.6.1 and the fact $\sigma_{-n} = \tau_n$ yield

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

Hence

$$\begin{aligned}(W_n &+ \delta C_n)(W_{n+m} + \delta C_{n+m}) = 4R^{2n+m}(\sigma_{2n+m} + \tau_n\sigma_m - \tau_{n-m}) \\ &= 4R^{2n+m}\left(\frac{W_{2n+m} + \delta C_{2n+m}}{2R^{2n+m}} + \frac{W_n - \delta C_n}{2R^n}\frac{W_m + \delta C_m}{2R^m} - \frac{W_{n-m} - \delta C_{n-m}}{2R^{n-m}}\right) \\ &= 2W_{2n+m} + 2\delta C_{2n+m} + R^n(W_nW_m - \delta C_nW_m + \delta C_mW_n - \Delta C_nC_m \\ &- 2R^{2m}W_{n-m} + 2\delta R^{2m}C_{n-m}).\end{aligned}$$

Thus we may conclude

$$\begin{aligned} W_nW_{n+m} &+ \delta C_nW_{n+m} + \delta C_{n+m}W_n + \Delta C_nC_{n+m} \\ &= 2W_{2n+m} + 2\delta C_{2n+m} + \delta R^n(-C_nW_m + C_mW_n + 2R^{2m}C_{n-m}) \\ &+ R^n(W_nW_m - \Delta C_nC_m - 2R^{2m}W_{n-m}). \end{aligned}$$

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 τ in Corollary 3.6.1. By adding and subtracting the resulting formula from that given above, we get

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

and

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

□

There are the following special cases of the previous theorem.

Corollary 3.10.1.

$$\begin{aligned} 2W_{2n} &= \Delta C_n^2 + W_n^2 - 4R^nW_n, \\ C_{2n} &= C_n(W_n + 2R^n) = C_nL_n, \\ 4W_{3n} &= 3\Delta C_n^2(W_n + 2R^n) + W_n^2(W_n - 6R^n) + 24R^{3n}, \\ 4C_{3n} &= C_n(\Delta C_n^2 + 3W_n^2). \end{aligned}$$

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 3.10.2.

$$2W_{n+3m} = \Delta C_m C_{n+2m} + W_m W_{n+2m} - R^m W_m W_{n+m} + R^m \Delta C_m C_{n+m} + 2R^{3m} W_n$$

$$2C_{n+3m} = W_m C_{n+2m} + C_m W_{n+2m} - R^m W_m C_{n+m} + R^m C_m W_{n+m} - 2R^{3m} C_n.$$

Proof. Use Theorem 3.10 and replace n by m and m by $n+m$. □

Theorem 3.11.

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

Proof. Replacing n with $n+r$ in the equations from Theorem 3.10 returns

$$\begin{aligned} 2W_{2n+2r+m} &= W_{n+r}W_{n+r+m} + \Delta C_{n+r}C_{n+r+m} \\ &- R^{n+r}(W_{n+r}W_m - \Delta C_{n+r}C_m - 2R^{2m}W_{n+r-m}) \end{aligned} \tag{3.7}$$

$$\begin{aligned} 2C_{2n+2r+m} &= C_{n+r+m}W_{n+r} + C_{n+r}W_{n+r+m} \\ &- R^{n+r}(C_m W_{n+r} - C_{n+r}W_m + 2R^{2m}C_{n+r-m}). \end{aligned} \tag{3.8}$$

Put $m = -r$ in (3.7) and (3.8) to obtain

$$\begin{aligned} 2W_{2n+r} &= W_{n+r}W_n + \Delta C_{n+r}C_n \\ &- R^{n+r}(W_{n+r}W_{-r} - \Delta C_{n+r}C_{-r} - 2R^{-2r}W_{n+2r}) \end{aligned}$$

$$\begin{aligned} 2C_{2n+r} &= C_n W_{n+r} + C_{n+r}W_n \\ &- R^{n+r}(C_{-r}W_{n+r} - C_{n+r}W_{-r} + 2R^{-2r}C_{n+2r}). \end{aligned}$$

Then use $W_{-r} = W_r/R^{2r}$, $C_{-r} = -C_r/R^{2r}$ to get

$$\begin{aligned} 2W_{2n+r} &= W_{n+r}W_n + \Delta C_{n+r}C_n \\ &- R^{n-r}W_{n+r}W_r - R^{n-r}\Delta C_{n+r}C_r + 2R^{n-r}W_{n+2r} \end{aligned} \tag{3.9}$$

$$\begin{aligned} 2C_{2n+r} &= C_nW_{n+r} + C_{n+r}W_n \\ &- R^{n-r}C_rW_{n+r} + R^{n-r}C_{n+r}W_r - 2R^{n-r}C_{n+2r}. \end{aligned} \tag{3.10}$$

Setting $m = 0$ in (3.7) and (3.8) we get

$$2W_{2n+2r} = W_{n+r}^2 + \Delta C_{n+r}^2 - (W_0 - 2)R^{n+r}W_{n+r} \tag{3.11}$$

$$2C_{2n+2r} = 2W_{n+r}C_{n+r} + (W_0 - 2)R^{n+r}C_{n+r}. \tag{3.12}$$

If we put $m = n$ in (3.8) and $m = n + 2r$ in the second identity in Theorem 3.10 we get

$$2C_{3n+2r} = W_{n+r}C_{2n+r} + C_{n+r}W_{n+2r} - R^{n+r}W_{n+r}C_n + R^{n+r}C_{n+r}W_n - 2R^{3n+r}C_r$$

$$2C_{3n+2r} = W_nC_{2n+2r} + C_nW_{2n+2r} - R^nW_nC_{n+2r} + R^nC_nW_{n+2r} + 2R^{3n}C_{2r}.$$

It follows by equating the right hand sides of the previous two equations and doubling that

$$\begin{aligned} 2W_{n+r}C_{2n+r} &+2C_{n+r}W_{n+2r} - 2R^{n+r}W_{n+r}C_n + 2R^{n+r}C_{n+r}W_n - 4R^{3n+r}C_r \\ = \quad & 2W_nC_{2n+2r} + 2C_nW_{2n+2r} - 2R^nW_nC_{n+2r} + 2R^nC_nW_{n+2r} + 4R^{3n}C_{2r}. \end{aligned}$$

Rearrange this to obtain

$$\begin{aligned} & 4R^{3n}(C_{2r} + R^rC_r) \\ = \; & 2W_{n+r}C_{2n+r} + 2C_{n+r}W_{n+2r} - 2W_nC_{2n+2r} - 2C_nW_{2n+2r} \\ - \; & 2R^{n+r}(W_{n+r}C_n - C_{n+r}W_n) + 2R^n(W_nC_{n+2r} - C_nW_{n+2r}). \end{aligned} \tag{3.13}$$

Now, using (3.9) and (3.10), notice that

$$\begin{aligned}
& 2W_{n+r}C_{2n+r} + 2C_{n+r}W_{n+2r} \\
= \;& W_{n+r}(W_{n+r}C_n + C_{n+r}W_n + R^{n-r}W_{n+r}C_r + R^{n-r}C_{n+r}W_r - 2R^{n-r}C_{n+2r}) \\
+ \;& C_{n+r}(W_{n+r}W_n + \Delta C_{n+r}C_n - R^{n-r}W_{n+r}W_r - R^{n-r}\Delta C_{n+r}C_r + 2R^{n-r}W_{n+2r}) \\
= \;& C_n(W_{n+r}^2 + \Delta C_{n+r}^2) + 2W_nW_{n+r}C_{n+r} + R^{n-r}(W_{n+r}^2 - \Delta C_{n+r}^2)C_r \\
+ \;& 2R^{n-r}(W_{n+2r}C_{n+r} - C_{n+2r}W_r).
\end{aligned}$$

Similarly by (3.11) and (3.12)

$$\begin{aligned}
& 2W_nC_{2n+2r} + 2C_nW_{2n+2r} \\
= \;& C_n(W_{n+r}^2 + \Delta C_{n+r}^2) + 2W_nW_{n+r}C_{n+r} + R^{n+r}(W_0 - 2)(W_nC_{n+r} - C_nW_{n+r}).
\end{aligned}$$

Using the last two identities we see

$$\begin{aligned}
& 2W_{n+r}C_{2n+r} + 2C_{n+r}W_{n+2r} - 2W_nC_{2n+2r} - 2C_nW_{2n+2r} \\
= \;& R^{n-r}(W_{n+r}^2 - \Delta C_{n+r}^2)C_r + 2R^{n-r}(W_{n+2r}C_{n+r} - C_{n+2r}W_r) \\
+ \;& R^{n+r}(W_0 - 2)(C_nW_{n+r} - W_nC_{n+r}).
\end{aligned}$$

Now use the above to modify (3.13) as follows

$$\begin{aligned}
& 4R^{3n}(C_{2r} + R^rC_r) \\
= \;& R^{n-r}(W_{n+r}^2 - \Delta C_{n+r}^2)C_r + 2R^{n-r}(W_{n+2r}C_{n+r} - C_{n+2r}W_r) \\
+ \;& R^{n+r}(W_0 - 2)(C_nW_{n+r} - W_nC_{n+r}) - 2R^{n+r}(W_{n+r}C_n - C_{n+r}W_n) \\
+ \;& 2R^n(W_nC_{n+2r} - C_nW_{n+2r}) \\
= \;& R^{n-r}(W_{n+r}^2 - \Delta C_{n+r}^2)C_r + 2R^{n-r}(W_{n+2r}C_{n+r} - C_{n+2r}W_r) \\
+ \;& R^{n+r}(W_0 - 4)(C_nW_{n+r} - W_nC_{n+r}) + 2R^n(W_nC_{n+2r} - C_nW_{n+2r}).
\end{aligned}$$

Dividing both sides of this equation by R^{n-r} gives

$$\begin{aligned} & 4R^{2n+r}(C_{2r} + R^r C_r) \\ = \; & (W_{n+r}^2 - \Delta C_{n+r}^2)C_r + 2(W_{n+2r}C_{n+r} - C_{n+2r}W_r) \\ + \; & R^{2r}(W_0 - 4)(C_n W_{n+r} - W_n C_{n+r}) - 2R^r(C_n W_{n+2r} - W_n C_{n+2r}). \quad (3.14) \end{aligned}$$

Putting $r = 1$ and replacing n by $n - 1$ in (3.14) yields

$$\begin{aligned} 4R^{2n-1}(C_2 + RC_1) &= W_n^2 - \Delta C_n^2 + 2(W_{n+1}C_n - C_{n+1}W_n) - 2R(W_{n+1}C_{n-1} \\ &- W_{n-1}C_{n+1}) + R^2(W_0 - 4)(W_n C_{n-1} - W_{n-1}C_n). \end{aligned}$$

Noting $C_2 = W_1 + 2R$, $W_1 = PQ - 3R$, $W_0 = 6$ and $C_1 = 1 \Rightarrow C_2 + RC_1 = PQ$ completes the proof. □

This formula is an extension the Lucas identity (2.11)

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

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

$$-2Q'^n = V_{n+1}U_n - U_{n+1}V_n \quad \text{when } m = n+1 \text{ and } n = n,$$

$$-2Q'^{n-1} = V_n U_{n-1} - U_n V_{n-1} \quad \text{when } m = n \text{ and } n = n-1,$$

$$-2Q'^{n-1}P' = V_{n+1}U_{n-1} - U_{n+1}V_{n-1} \quad \text{when } m = n+1 \text{ and } n = n-1.$$

Replacing Q' by R^2 in the above returns

$$V_{n+1}U_n - U_{n+1}V_n = -2R^{2n},$$
$$V_nU_{n-1} - U_nV_{n-1} = -2R^{2n-2},$$
$$V_{n+1}U_{n-1} - U_{n+1}V_{n-1} = -2R^{2n-2}P'.$$

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 3.11 we see

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

It is not surprising that Theorem 3.11 involves 6 objects: W_{n-1}, W_n, W_{n+1}, C_{n-1}, C_n, C_{n+1}, as one may recall that both $\{W_n\}$ and $\{C_n\}$ satisfy a degree 6 recurrence.

By similar methods we can develop and justify another generalization of the same Lucas identity $V_n^2 - \Delta U_n^2 = 4Q'^n$ in the following theorem.

Theorem 3.12.

$$\begin{aligned} &4R^{2n-1}(P^2Q^2 - 2Q^3 - 2RP^3 + 5PQR - 6R^2) = \\ &\quad -(W_n^2 - \Delta C_n^2)W_1 + 2(W_{n+1}W_n - \Delta C_{n+1}C_n) + 2R(W_{n+1}W_{n-1} - \Delta C_{n-1}C_{n+1}) \\ &\quad +2R^2(W_nW_{n-1} - \Delta C_{n-1}C_n). \end{aligned}$$

Proof. If we put $m = n$ in (3.7) and $m = n + 2r$ in the first identity of Theorem 3.10 we get

$$\begin{aligned} 2W_{3n+r} &= W_{n+r}W_{2n+r} + \Delta C_{n+r}C_{2n+r} \\ &- R^{n+r}W_{n+r}W_n + R^{n+r}\Delta C_{n+r}C_n + 2R^{3n+r}W_r \end{aligned}$$

$$\begin{aligned} 2W_{3n+r} &= W_nW_{2n+2r} + \Delta C_nC_{2n+2r} \\ &- R^nW_{n+2r}W_n + R^n\Delta C_{n+2r}C_n + 2R^{3n}W_{2r}. \end{aligned}$$

Equate the right hand sides, double, then rearrange to obtain

$$\begin{aligned} 4R^{3n}(W_{2r} - R^rW_r) &= 2W_{n+r}W_{2n+r} + 2\Delta C_{n+r}C_{2n+r} - 2W_nW_{2n+2r} - 2\Delta C_nC_{2n+2r} \\ &- 2R^{n+r}(W_{n+r}W_n - \Delta C_{n+r}C_n) \\ &+ 2R^n(W_{n+2r}W_n - \Delta C_{n+2r}C_n). \end{aligned} \tag{3.15}$$

Similarly, use (3.9) and (3.10) to see

$$\begin{aligned} & 2W_{n+r}W_{2n+r} + 2\Delta C_{n+r}C_{2n+r} \\ = \; & (W_{n+r}^2 + \Delta C_{n+r}^2)W_n + 2\Delta W_{n+r}C_{n+r}C_n - R^{n-r}(W_{n+r}^2 - \Delta C_{n+r}^2)W_r \\ + \; & 2R^{n-r}(W_{n+2r}W_{n+r} - \Delta C_{n+r}C_{n+2r}). \end{aligned}$$

By (3.11) and (3.12) we have

$$\begin{aligned} & 2W_nW_{2n+2r} + 2\Delta C_nC_{2n+2r} \\ = \; & W_n(W_{n+r}^2 + \Delta C_{n+r}^2) + 2\Delta W_{n+r}C_{n+r}C_n \\ - \; & (W_0 - 2)R^{n+r}(W_nW_{n+r} - \Delta C_nC_{n+r}). \end{aligned}$$

Using (3.15) and the above, we have

$$\begin{aligned} 4R^{2n+r}(W_{2r} + R^rW_r) &= -(W_{n+r}^2 - \Delta C_{n+r}^2)W_r + 2(W_{n+2r}W_{n+r} - \Delta C_{n+2r}C_{n+r}) \\ &+ 2R(W_{n+2r}W_n - \Delta C_{n+2r}C_n) + R^{2r}(W_0 - 4) \\ &\quad (W_{n+r}W_n - \Delta C_{n+r}C_n). \end{aligned}$$

Using the above and replacing r by 1 and n by $n-1$ we have

$$\begin{aligned} 4R^{2n-1}(W_2+RW_1) &= -(W_n^2-\Delta C_n^2)W_1+2(W_{n+1}W_n-\Delta C_{n+1}C_n)+2R(W_{n+1}W_{n-1} \\ &- \Delta C_{n-1}C_{n+1})+R^2(W_0-4)(W_nW_{n-1}-\Delta C_{n-1}C_n). \end{aligned}$$

Using the identities $W_2=\frac{1}{2}\Delta+\frac{1}{2}W_1^2-2RW_1$ and $W_1=PQ-3R$ to show $W_2+RW_1=P^2Q^2-2Q^3-2RP^3+5PQR-6R^2$ completes the proof. □

The formula from the above theorem is another logical extension of the Lucas identity

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

where $V_n=V_n(P',Q')$ and $U_n=U_n(P',Q')$. Again, 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

$$2Q'^mV_{n-m}=V_nV_m-\Delta U_nU_m$$

we can see

$$\begin{aligned} 2Q'^nV_1 &= V_{n+1}V_n-\Delta U_{n+1}U_n \quad \text{when } m=n \text{ and } n=n+1, \\ 2Q'^{n-1}V_2 &= V_{n+1}V_{n-1}-\Delta U_{n+1}U_{n-1} \quad \text{when } m=n-1 \text{ and } n=n+1, \\ 2Q'^{n-1}V_1 &= V_nV_{n-1}-\Delta U_nU_{n-1} \quad \text{when } m=n-1 \text{ and } n=n. \end{aligned}$$

Again, replace Q' by R^2 in the above to obtain

$$\begin{aligned} V_{n+1}V_n-\Delta U_{n+1}U_n &= 2R^{2n}V_1, \\ V_{n+1}V_{n-1}-\Delta U_{n+1}U_{n-1} &= 2R^{2n-2}V_2, \\ V_nV_{n-1}-\Delta U_nU_{n-1} &= 2R^{2n-2}V_1. \end{aligned}$$

It is easily verified that $V_2 - RV_1 = P'^2 - 2R^2 - RP'$. The above facts and replacing W_m by V_m and C_m by U_m into the equation in Theorem 3.12 yield

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

Replacing R^2 with Q' and dividing both sides by P' completes the analogy, giving

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

In view of the importance that the quantity $W_n - 6R^n$ will assume in later chapters, we also point out that from Theorem 3.3 it is easy to deduce that

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

3.5 Multiplication Formulas for W_n and C_n

Theorem 3.13.

$$\begin{aligned} 16C_{5n}/C_n &= \Delta^2 C_n^4 + 20R^{2n}\Delta C_n^2 + 20R^n \Delta C_n^2 W_n + 10\Delta C_n^2 W_n^2 + 80R^{3n}W_n \\ &\quad -20R^{2n}W_n^2 - 20R^n W_n^3 + 5W_n^4 + 80R^{4n}, \\ 16W_{5n} &= 5\Delta^2 C_n^4(W_n + 2R^n) + 10\Delta C_n^2(W_n^3 - 2R^{2n}W_n + 4R^{3n}) + W_n(W_n^4 \\ &\quad -10R^n W_n^3 + 20R^{2n}W_n^2 + 40R^{3n}W_n - 80R^{4n}). \end{aligned}$$

Proof. Replace σ_n and τ_n with the equations in (3.4) and place them in the first

identity from Corollary 3.7.1 to see

$$\begin{aligned}\frac{W_{5n}+\delta C_{5n}}{2R^{5n}} &= \left(\frac{W_n+\delta C_n}{2R^n}\right)^5 - 5\left(\frac{W_n+\delta C_n}{2R^n}\right)^3\left(\frac{W_n-\delta C_n}{2R^n}\right) \\ &+ 5\left(\frac{W_n+\delta C_n}{2R^n}\right)\left(\frac{W_n-\delta C_n}{2R^n}\right)^2 + 5\left(\frac{W_n+\delta C_n}{2R^n}\right)^2 - 5\left(\frac{W_n-\delta C_n}{2R^n}\right).\end{aligned}$$

Multiply both sides by $32R^{5n}$ to see

$$\begin{aligned}16(W_{5n}+\delta C_{5n}) &= (W_n+\delta C_n)^5 - 10R(W_n+\delta C_n)^3(W_n-\delta C_n) + 20R^{2n}(W_n+\delta C_n) \\ &\quad (W_n-\delta C_n)^2 + 40R^{3n}(W_n+\delta C_n)^2 - 80R^{4n}(W_n-\delta C_n) \\ &= W_n^5 + 5\delta W_n^4 C_n + 10\Delta W_n^3 C_n^2 + 10\delta\Delta W_n^2 C_n^3 + 5\Delta^2 W_n C_n^4 + \delta\Delta^2 C_n^5 \\ &\quad -10R(W_n^4 - \Delta^2 C_n^4) + 20R^{2n}(W_n^3 - \Delta W_n C_n^2 - \delta W_n^2 C_n + \delta\Delta C_n^3) \\ &\quad +40R^{3n}(W_n^3 + \Delta C_n^2 + 2\delta W_n C_n) - 80R^{4n}(W_n - \delta C_n).\end{aligned}$$

Equating the irrational parts and rearranging completes the proof. If $\delta \in \mathbb{Z}$, then we may use $\frac{W_{5n}-\delta C_{5n}}{2R^{5n}}$ and the second identity from Corollary 3.7.1 to complete the proof. □

A more general multiplicative result is shown in the following theorem and this result is our analogue to (2.14) and (2.15). 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.

Theorem 3.14. *For any integers $m \geq 0$ we have*

$$W_{mn} = \sum \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(\lambda_0+\lambda_3)} \tilde{Q}_n^{\lambda_2} V_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) \qquad (3.16)$$

$$\frac{C_{mn}}{C_n} = \sum \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(\lambda_0+\lambda_3)} \tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n). \qquad (3.17)$$

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

$$\lambda_0, \lambda_1, \lambda_2, \lambda_3 \geq 0, \quad \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = m, \quad \lambda_1 + 2\lambda_2 + 3\lambda_3 = m,$$

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

Proof. First note $\sigma_1 = \alpha/\beta + \beta/\gamma + \gamma/\alpha = \sum r_i$, where the sum is over the three quantities $r_1 = \alpha/\beta$, $r_2 = \beta/\gamma$, and $r_3 = \gamma/\alpha$. Thus σ_1 is the first elementary function of degree three involving these three terms. Also $\tau_1 = \beta/\alpha + \gamma/\beta + \alpha/\gamma = \sum_{i \neq j} r_i r_j$. Thus τ_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

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

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

$$\sigma_{mn} = \sum_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} (-1)^{\lambda_0} \frac{m(m - \lambda_0 - 1)!}{\lambda_1! \lambda_2! \lambda_3!} \sigma_n^{\lambda_1} \tau_n^{\lambda_2}, \tag{3.18}$$

$$\tau_{mn} = \sum_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} (-1)^{\lambda_0} \frac{m(m - \lambda_0 - 1)!}{\lambda_1! \lambda_2! \lambda_3!} \tau_n^{\lambda_1} \sigma_n^{\lambda_2}, \tag{3.19}$$

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,

$$\begin{aligned} S_n^{\lambda} &= \left(\frac{W_n + \delta C_n}{2}\right)^{\lambda} = \frac{V_\lambda + \tilde{\delta}_n U_\lambda}{2}, \\ T_n^{\lambda} &= \left(\frac{W_n - \delta C_n}{2}\right)^{\lambda} = \frac{V_\lambda - \tilde{\delta}_n U_\lambda}{2}, \end{aligned}$$

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 the first identity, 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

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

The second identity is proven similarly by expanding $\delta C_n = S_n - T_n$ via Waring's theorem as follows,

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

Now, using substitutions for the U, V as before,

$$\begin{aligned} R^{mn}(\sigma_n^{\lambda_1}\tau_n^{\lambda_2} - \sigma_n^{\lambda_2}\tau_n^{\lambda_1}) &= R^{(m-\lambda_1-\lambda_2)n}(R^{n\lambda_1}\sigma_n^{\lambda_1}R^{n\lambda_2}\tau_n^{\lambda_2} - R^{n\lambda_2}\sigma_n^{\lambda_2}R^{n\lambda_1}\tau_n^{\lambda_1}) \\ &= R^{(\lambda_0+\lambda_3)n}(S_n^{\lambda_1}T_n^{\lambda_2} - S_n^{\lambda_2}T_n^{\lambda_1}) \\ &= \frac{V_{\lambda_1} + \tilde{\delta}_n U_{\lambda_1}}{2}\frac{V_{\lambda_2} - \tilde{\delta}_n U_{\lambda_2}}{2} - \frac{V_{\lambda_2} + \tilde{\delta}_n U_{\lambda_2}}{2}\frac{V_{\lambda_1} - \tilde{\delta}_n U_{\lambda_1}}{2} \\ &= \frac{\tilde{\delta}_n}{2}(U_{\lambda_1}V_{\lambda_2} - U_{\lambda_2}V_{\lambda_1}). \end{aligned}$$

Again, we will use an identity for Lucas sequences to complete the proof,

$$U_{\lambda_1}V_{\lambda_2} - U_{\lambda_2}V_{\lambda_1} = 2\tilde{Q}_n^{\lambda_2}U_{\lambda_1-\lambda_2}$$

and we replace $\tilde{\delta}_n$ by δC_n. □

The corollary below states some special cases.

Corollary 3.14.1.

$$\begin{aligned} C_{5n}/C_n &= 5R^{4n} + 5R^{3n}\tilde{P}_n - 5R^{2n}\tilde{Q}_n - 5R^n\tilde{P}_n\tilde{Q}_n + \tilde{P}_n^4 - 3\tilde{P}_n^2\tilde{Q}_n + \tilde{Q}_n^2, \\ C_{6n}/C_n &= 8R^{3n}(\tilde{P}_n^2 - \tilde{Q}_n) - 6R^n\tilde{Q}_n(\tilde{P}_n^2 - \tilde{Q}_n) + \tilde{P}_n^5 - 4\tilde{P}_n^3\tilde{Q}_n + 3\tilde{P}_n\tilde{Q}_n^2, \\ C_{7n}/C_n &= 7R^{6n} - 7R^{5n}\tilde{P}_n - 21R^{4n}\tilde{Q}_n + 7R^{3n}\tilde{P}_n(\tilde{P}_n^2 - \tilde{Q}_n) + 14R^{2n}\tilde{Q}_n^2 \\ &\quad + 7R^n\tilde{P}_n\tilde{Q}_n(2\tilde{Q}_n - \tilde{P}_n^2) + \tilde{P}_n^6 - 5\tilde{P}_n^4\tilde{Q}_n + 6\tilde{P}_n^2\tilde{Q}_n^2 - \tilde{Q}_n^3. \end{aligned}$$

It is of interest that we can use the multiplicative identity for C_{mn} to show we may calculate C_m as a sum of Lucas sequences.

Corollary 3.14.2.

$$C_m = m \sum_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{(-1)^{\lambda_0}(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{\lambda_0+\lambda_3} \tilde{Q}_1^{\lambda_2} U_{\lambda_1-\lambda_2}(\tilde{P}_1, \tilde{Q}_1),$$

where $\tilde{P}_1 = PQ - 3R$ *and* $\tilde{Q}_1 = (\tilde{P}_1^2 - \Delta)/4 = RP^3 + Q^3 - 6PQR + 9R^2$.

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 Chapter 4. Once we have arithmetic properties some primality testing can be done.

3.6 Calculating Generalized Lucas Sequences

By Theorem 3.8 we know that both the $\{W_n\}$ and $\{C_n\}$ sequences satisfy the recurrence formula

$$Z_{nm+6n} = a_1 Z_{nm+5n} - a_2 Z_{nm+4n} + a_3 Z_{nm+3n} - a_4 Z_{nm+2n} + a_5 Z_{nm+n} - a_6 Z_{nm},$$

where

$$\begin{aligned} &a_1 = W_n, \quad a_2 = (W_n^2 - \Delta C_n^2)/4 + R^n W_n, \\ &a_3 = R^n(W_{2n} + 2R^n W_n + 2R^{2n}), \quad a_4 = R^{2n} a_2, \\ &a_5 = R^{4n} a_1, \quad a_6 = R^{6n}. \end{aligned}$$

Also, we have in Corollary 3.10.1 the result that $2W_{2n} = \Delta C_n^2 + W_n^2 - 4R^n W_n$. Now put

$$X_k = \frac{W_k}{2R^k} \quad \text{and} \quad \tilde{D}_k = \frac{\tilde{\Delta}_k}{4R^{2k}} = \frac{\Delta C_k^2}{4R^{2k}},$$

then

$$\frac{a_1}{R^n} = 2X_n, \quad \frac{a_2}{R^{2n}} = \frac{(W_n^2 - \Delta C_n^2)}{4R^{2n}} + \frac{R^n W_n}{R^{2n}} = X_n^2 + 2X_n - \tilde{D}_n,$$

$$\begin{aligned}
\frac{a_3}{R^{3n}} &= \frac{R^n(W_{2n} + 2R^n W_n + 2R^{2n})}{R^{3n}} = \frac{W_{2n}}{R^{2n}} + \frac{2W_n}{R^n} + 2 \\
&= \frac{\Delta C_n^2 + W_n^2 - 4R^n W_n}{2R^{2n}} + \frac{2W_n}{R^n} + 2 = \frac{\Delta C_n^2 + W_n^2}{2R^{2n}} - \frac{2W_n}{R^n} + \frac{2W_n}{R^n} + 2 \\
&= 2\frac{\Delta C_n^2}{4R^{2n}} + 2\frac{W_n^2}{4R^{2n}} + 2 = 2(X_n^2 + \tilde{D}_n + 1),
\end{aligned}$$

$$\begin{aligned}
\frac{a_4}{R^{4n}} &= \frac{R^{2n} a_2}{R^{4n}} = \frac{a_2}{R^{2n}} = X_n^2 + 2X_n - \tilde{D}_n, \quad \frac{a_5}{R^{5n}} = \frac{R^{4n} a_1}{R^{5n}} = \frac{a_1}{R^n} = 2X_n, \\
\frac{a_6}{R^{6n}} &= 1.
\end{aligned}$$

Hence

$$\begin{aligned}
X_{(m+6)n} &= 2X_n X_{(m+5)n} - (X_n^2 - \tilde{D}_n + 2X_n) X_{(m+4)n} + 2(X_n^2 + \tilde{D}_n + 1) X_{(m+3)n} \\
&- (X_n^2 - \tilde{D}_n + 2X_n) X_{(m+2)n} + 2X_n X_{(m+1)n} - X_{mn},
\end{aligned}$$

where

$$\begin{aligned}
X_0 &= 3, \quad X_n = \frac{W_n}{2R^n}, \quad X_{2n} = \frac{W_{2n}}{2R^{2n}} = \frac{\Delta C_n^2 + W_n^2 - 4R^n W_n}{4R^{2n}} = X_n^2 + \tilde{D}_n - 2X_n, \\
X_{3n} &= \frac{W_{3n}}{2R^{3n}} = \frac{W_n^3}{8R^{3n}} + 3\frac{\Delta C_n^2 W_n}{8R^{3n}} + 3\frac{R^n \Delta C_n^2}{4R^{3n}} - 3\frac{R^n W_n^2}{4R^{3n}} + \frac{6R^{3n}}{2R^{3n}} \\
&= \frac{W_n^3}{8R^{3n}} + 3\frac{\Delta C_n^2}{4R^{2n}}\frac{W_n}{2R^n} + 3\frac{\Delta C_n^2}{4R^{2n}} - 3\frac{W_n^2}{4R^{2n}} + 3 \\
&= X_n^3 + 3\tilde{D}_n X_n + 3\tilde{D}_n - 3X_n^2 + 3.
\end{aligned}$$

Also,

$$X_{-mn} = \frac{W_{-mn}}{2R^{-mn}} = \frac{W_{mn}}{R^{2(mn)}} / 2R^{-mn} = \frac{W_{mn}}{2R^{mn}} = X_{mn}.$$

It follows that $X_{mn} = F_m(X_n, \tilde{D}_n)$, where

$$\begin{aligned}
F_{m+6} &= 2X_n F_{m+5} - (X_n^2 - \tilde{D}_n + 2X_n) F_{m+4} + 2(X_n^2 + \tilde{D}_n + 1) F_{m+3} \\
&- (X_n^2 - \tilde{D}_n + 2X_n) F_{m+2} + 2X_n F_{m+1} - F_m,
\end{aligned}$$

and

$$\begin{aligned} F_0 &= 3, \quad F_1 = X_n, \quad F_2 = X_n^2 + \tilde{D}_n - 2X_n, \quad F_3 = X_n^3 + 3\tilde{D}_n X_n + 3\tilde{D}_n - 3X_n^2 + 3, \\ & F_m(X_n, \tilde{D}_n) = F_{-m}(X_n, \tilde{D}_n). \end{aligned}$$

Furthermore, if we put $Y_{m,n} = \frac{C_{mn}}{C_n R^{mn-n}}$, then $Y_{m,n} = G_m(X_n, \tilde{D}_n)$ where

$$\begin{aligned} G_{m+6} &= 2X_n G_{m+5} - (X_n^2 - \tilde{D}_n + 2X_n)G_{m+4} + 2(X_n^2 + \tilde{D}_n + 1)G_{m+3} \\ &- (X_n^2 - \tilde{D}_n + 2X_n)G_{m+2} + 2X_n G_{m+1} - G_m, \end{aligned}$$

and

$$\begin{aligned} G_0 &= 0, \quad G_1 = Y_{1,n} = \frac{C_n}{C_n R^{1-1}} = 1, \\ G_2 &= \frac{C_{2n}}{C_n R^n} = \frac{C_n W_n}{C_n R^n} + \frac{2R^n C_n}{C_n R^n} = 2X_n + 2, \\ G_3 &= \frac{C_{3n}}{C_n R^{2n}} = \frac{3C_n W_n^2}{4C_n R^{2n}} + \frac{\Delta C_n^3}{4C_n R^{2n}} = \frac{3W_n^2}{4R^{2n}} + \frac{\Delta C_n^2}{4R^{2n}} = 3X_n^2 + \tilde{D}_n. \end{aligned}$$

Also,

$$Y_{-m,n} = \frac{C_{-mn}}{C_n R^{-mn-n}} = \frac{-C_{mn}}{R^{2mn}} / C_n R^{-mn-n} = -\frac{C_{mn} R^{mn+n}}{C_n R^{2mn}} = -\frac{C_{mn}}{C_n R^{mn-n}} = -Y_{m,n}.$$

So

$$G_m(X_n, \tilde{D}_n) = -G_{-m}(X_n, \tilde{D}_n).$$

Note that

$$\tilde{D}_{mn} = \frac{\Delta C_{mn}^2}{4R^{2mn}} = \Delta \frac{C_n^2}{C_n^2} \frac{C_{mn}^2}{4R^{2mn}} = \frac{\Delta C_n^2}{4R^{2n}} \frac{C_{mn}^2}{C_n^2 (R^{mn-n})^2} = \tilde{D}_n G_m^2.$$

Thus we have found that if we put

$$X_n = \frac{W_n}{2R^n}, \quad \tilde{D}_n = \frac{\Delta C_n^2}{4R^{2n}} \quad \text{and} \quad Y_{m,n} = \frac{C_{mn}}{C_n R^{mn-n}},$$

then

$$X_{mn} = F_m(X_n, \tilde{D}_n), \quad Y_{m,n} = G_m(X_n, \tilde{D}_n),$$

where F_m, $G_m \in \mathbb{Z}[x, y]$ satisfy

$$\begin{aligned} Z_{m+6} &= 2xZ_{m+5} - (x^2 + 2x - y)Z_{m+4} + 2(x^2 + y + 1)Z_{m+3} \\ &- (x^2 + 2x - y)Z_{m+2} + 2xZ_{m+1} - Z_m, \end{aligned} \tag{3.20}$$

and

$$\begin{aligned} F_0 &= 3, \quad F_1 = x, \quad F_2 = x^2 - 2x + y, \quad F_3 = x^3 + 3yx + 3y - 3x^2 + 3, \\ G_0 &= 0, \quad G_1 = 1, \quad G_2 = 2x + 2, \quad G_3 = 3x^2 + y, \end{aligned}$$

$$F_{-m}(x, y) = F_m(x, y) \quad \text{and} \quad G_{-m}(x, y) = -G_m(x, y).$$

Consider the equation

$$z^3 - (x + \sqrt{y})z^2 + (x - \sqrt{y})z - 1 = 0. \tag{3.21}$$

Let λ, μ, ν be the zeros of (3.21). Then clearly λ^{-1}, μ^{-1}, ν^{-1} are the zeros of

$$z^3 - (x - \sqrt{y})z^2 + (x + \sqrt{y})z - 1 = 0$$

and therefore λ, μ, ν, λ^{-1}, μ^{-1}, ν^{-1} are the zeros of

$$(z^3 - (x + \sqrt{y})z^2 + (x - \sqrt{y})z - 1)(z^3 - (x - \sqrt{y})z^2 + (x + \sqrt{y})z - 1)$$

$$= z^6 - 2xz^5 + (x^2 + 2x - y)z^4 - (2x^2 + 2y + 2)z^3 + (x^2 + 2x - y)z^2 - 2xz + 1.$$

Note that $\lambda\mu\nu = 1$. From this, the boundary conditions on F_m and G_m and the fact that they satisfy the recurrence (3.20), we find that

$$F_m = F_m(x, y) = \frac{1}{2}(\lambda^m + \mu^m + \nu^m + \lambda^{-m} + \mu^{-m} + \nu^{-m}),$$

$$G_m = G_m(x,y) = \frac{\lambda^m + \mu^m + \nu^m - \lambda^{-m} - \mu^{-m} - \nu^{-m}}{2\sqrt{y}} \quad \text{for} \quad y \neq 0.$$

Since λ, μ, ν satisfy

$$\begin{aligned} z^{n+3} &= (x+\sqrt{y})z^{n+2} - (x-\sqrt{y})z^{n+1} + z^n, \\ z^{-(n+3)} &= (x-\sqrt{y})z^{-(n+2)} - (x+\sqrt{y})z^{-(n+1)} + z^{-n}, \end{aligned}$$

we can see that

$$\begin{aligned} F_{n+3} &= \frac{1}{2}(\lambda^{n+3} + \mu^{n+3} + \nu^{n+3} + \lambda^{-(n+3)} + \mu^{-(n+3)} + \nu^{-(n+3)}) \\ &= \frac{1}{2}((x+\sqrt{y})\lambda^{n+2} - (x-\sqrt{y})\lambda^{n+1} + \lambda^n + (x+\sqrt{y})\mu^{n+2} \\ &\quad -(x-\sqrt{y})\mu^{n+1} + \mu^n + (x+\sqrt{y})\nu^{n+2} - (x-\sqrt{y})\nu^{n+1} \\ &\quad +\nu^n + (x-\sqrt{y})\lambda^{-(n+2)} - (x+\sqrt{y})\lambda^{-(n+1)} + \lambda^{-n} \\ &\quad +(x-\sqrt{y})\mu^{-(n+2)} - (x+\sqrt{y})\mu^{-(n+1)} + \mu^{-n} + (x-\sqrt{y})\nu^{-(n+2)} \\ &\quad -(x+\sqrt{y})\nu^{-(n+1)} + \nu^{-n}) \\ &= \frac{1}{2}(x\lambda^{n+2} + \sqrt{y}\lambda^{n+2} - x\lambda^{n+1} + \sqrt{y}\lambda^{n+1} + \lambda^n \\ &\quad +x\mu^{n+2} + \sqrt{y}\mu^{n+2} - x\mu^{n+1} + \sqrt{y}\mu^{n+1} + \mu^n \\ &\quad +x\nu^{n+2} + \sqrt{y}\nu^{n+2} - x\nu^{n+1} + \sqrt{y}\nu^{n+1} + \nu^n \\ &\quad +x\lambda^{-(n+2)} - \sqrt{y}\lambda^{-(n+2)} - x\lambda^{-(n+1)} - \sqrt{y}\lambda^{-(n+1)} + \lambda^{-n} \\ &\quad +x\mu^{-(n+2)} - \sqrt{y}\mu^{-(n+2)} - x\mu^{-(n+1)} - \sqrt{y}\mu^{-(n+1)} + \mu^{-n} \\ &\quad +x\nu^{-(n+2)} - \sqrt{y}\nu^{-(n+2)} - x\nu^{-(n+1)} - \sqrt{y}\nu^{-(n+1)} + \nu^{-n}) \\ &= xF_{n+2} - xF_{n+1} + yG_{n+2} + yG_{n+1} + F_n. \end{aligned}$$

By the same method one can easily verify that

$$G_{n+3} = xG_{n+2} - xG_{n+1} + F_{n+2} + F_{n+1} + G_n.$$

If we put $H_n = \lambda^n + \mu^n + \nu^n$ then by Theorem 3.6 we have that

$$H_{n+m} = H_n H_m - H_{-n} H_{m-n} + H_{m-2n}. \tag{3.22}$$

Putting $m = n + 1$ in equation (3.22), we get

$$H_{2n+1} = H_n H_{n+1} - H_{-n} H_1 + H_{-n+1}. \tag{3.23}$$

Now using the facts

$$F_n = \frac{1}{2}(H_n + H_{-n}) \quad \text{and} \quad G_n = \frac{1}{2\sqrt{y}}(H_n - H_{-n}),$$

yields

$$H_n = F_n + \sqrt{y} G_n \quad \text{and} \quad H_{-n} = F_n - \sqrt{y} G_n.$$

Substituting this into (3.23) we get

$$\begin{aligned} F_{2n+1} &= F_n F_{n+1} + y G_n G_{n+1} - x F_n + y G_n + F_{n-1}, \\ G_{2n+1} &= G_n F_{n+1} + G_{n+1} F_n + x G_n - F_n - G_{n-1}. \end{aligned}$$

Or more generally, using (3.22) and replacing m by $m + n$, we can derive

$$\begin{aligned} F_{2n+m} &= y G_n (G_{m+n} + G_m) + F_n (F_{m+n} - F_m) + F_{m-n}, \\ G_{2n+m} &= G_n (F_{m+n} + F_m) + F_n (G_{m+n} - G_m) + G_{m-n}. \end{aligned}$$

The cost of computing F_{2n+m}, G_{2n+m} from

$$\{F_{m+n}, G_{m+n}, F_m, G_m, F_n, G_n, F_{m-n}, G_{m-n}\}$$

is 5 multiplications.

Now since

$$\begin{aligned} F_{n+2} &= xF_{n+1} - xF_n + yG_{n+1} + yG_n + F_{n-1}, \\ G_{n+2} &= xG_{n+1} - xG_n + F_{n+1} + F_n + G_{n-1}, \end{aligned}$$

we get

$$\begin{aligned} F_{n-1} &= F_{n+2} - xF_{n+1} + xF_n - yG_{n+1} - yG_n, \\ G_{n-1} &= G_{n+2} - xG_{n+1} + xG_n - F_{n+1} - F_n. \end{aligned}$$

Hence

$$\begin{aligned} F_{2n+1} &= F_nF_{n+1} + yG_nG_{n+1} - xF_{n+1} - yG_{n+1} + F_{n+2} \\ &= F_{n+1}(F_n - x) + yG_{n+1}(G_n - 1) + F_{n+2}, \qquad (3.24) \\ G_{2n+1} &= G_nF_{n+1} + G_{n+1}F_n - G_{n+2} + xG_{n+1} + F_{n+1} \\ &= F_{n+1}(G_n + 1) + G_{n+1}(F_n + x) - G_{n+2}. \qquad (3.25) \end{aligned}$$

Also, if we replace n by $n + 1$ in the above, then

$$\begin{aligned} F_{2n+3} &= F_{n+1}(F_{n+2} - x) - yG_{n+1}(G_{n+2} - 1) + F_n, \qquad (3.26) \\ &= G_{2n+3} = F_{n+1}(G_{n+2} + 1) + G_{n+1}(F_{n+2} + x) - G_n. \qquad (3.27) \end{aligned}$$

We can also set $m = n$ in (3.22) to get

$$H_{2n} = H_n^2 - 3H_{-n} + H_{-n} = H_n^2 - 2H_{-n} \quad \text{and} \quad H_{-2n} = H_{-n}^2 - 2H_n.$$

Using this, we can easily obtain

$$F_{2n} = F_n^2 + yG_n^2 - 2F_n = F_n(F_n - 2) + yG_n^2, \tag{3.28}$$

$$G_{2n} = 2G_n(F_n + 1), \tag{3.29}$$

$$F_{2n+2} = F_{n+1}(F_{n+1} - 2) + yG_{n+1}^2, \tag{3.30}$$

$$G_{2n+2} = 2G_{n+1}(F_{n+1} + 1). \tag{3.31}$$

Thus given the sextet

$$S_n = \{F_n, F_{n+1}, F_{n+2}, G_n, G_{n+1}, G_{n+2}\}$$

we can compute

$$S_{2n+1} = \{F_{2n+1}, F_{2n+2}, F_{2n+3}, G_{2n+1}, G_{2n+2}, G_{2n+3}\}$$

using (3.24), (3.25), (3.26), (3.27), (3.30), (3.31) with 12 multiplications. If one is not careful it may appear as though we need to do 14 multiplications, but yG_{n+1} occurs 3 times and we need only calculate it once. We are also able to compute

$$S_{2n} = \{F_{2n}, F_{2n+1}, F_{2n+2}, G_{2n}, G_{2n+1}, G_{2n+2}\}$$

using (3.24), (3.25), (3.28), (3.29), (3.30), (3.31) with 12 multiplications.

These observations can now be used to compute (by F) X_{mn}, $Y_{m,n} \pmod r$ for a given modulus r, given X_n, $\tilde{D}_n$ in $O(\log m)$ modular multiplications. We begin with

$$S_1 = \{F_1, F_2, F_3, G_1, G_2, G_3\} \pmod r,$$

which can be computed using X_n, $\tilde{D}_n$ only. We then compute

$$S_m = \{F_m, F_{m+1}, F_{m+2}, G_m, G_{m+1}, G_{m+2}\} \pmod r$$

as follows. Let $(b_0 b_1 \dots b_k)_2 = m$ be the binary representation of m such that $b_0 \neq 0$. Set $\mathcal{P}_0 = S_1$ and for $i = 0$ to $i = k - 1$

$$\mathcal{P}_{i+1} = \begin{cases} S_{2n} \pmod r & \text{if } b_{i+1} = 0 \\ S_{2n+1} \pmod r & \text{if } b_{i+1} = 1. \end{cases}$$

Then $\mathcal{P}_k = S_m$. This gives us $X_{mn} \equiv F_m \pmod r$, $Y_{m,n} \equiv G_m \pmod r$ and $\tilde{D}_{mn} = \tilde{D}_n G_m^2 \pmod r$.

Thus, if $k = \lceil \log m \rceil$ we need to perform $12k$ modular multiplications to compute $S_m \pmod r$. To compute $t_m \equiv a^m \pmod r$ requires on average $\frac{3}{2}k$ modular multiplications. Thus, for a given m computing S_m is 8 times more expensive than computing t_m.

Chapter 4

Arithmetic Properties of $\{C_n\}$ and $\{W_n\}$

4.1 Introductory Arithmetic Results

To continue our generalization we need to develop arithmetic results, both global and local, that are logical analogues of the arithmetic results seen in Chapter 2 for Lucas sequences.

Lemma 4.1. *If* $(Q, R) = 1$, *then* $(B_n, R) = 1$, *for* $n > 0$.

Proof. First note $B_0 = 3$, $B_1 = Q$ and $B_2 = Q^2 - RP$. Also for $n \geq 0$

$$B_{n+3} = QB_{n+2} - RPB_{n+1} + R^2 B_n.$$

By induction $B_n \equiv Q^n \pmod{R}$ for $n > 0$. The result follows immediately. □

We also can produce a somewhat similar result which involves A_n instead of B_n.

Theorem 4.2. *If* $(Q, R) = 1$, *then* $(A_n, R, \Delta) \mid 4$.

Proof. Let p be any odd prime such that $p \mid (\Delta, R)$. From the formula for Δ, we see that $p \mid Q^2P^2 - 4Q^3$, and since $(Q, R) = 1$, we must have that $p \mid P^2 - 4Q$. Now $A_0 = 3$, $A_1 = P$, $A_2 = P^2 - 2Q$ and

$$A_{k+2} \equiv PA_{k+1} - QA_k \pmod{R}.$$

Since $Q \equiv P^2/4 \pmod{p}$, we get

$$A_n \equiv P^n/2^{n-1} \pmod{p}$$

by induction on n. Since $p \nmid P$, we have $p \nmid A_n$ and $p \nmid (A_n, R, \Delta)$.

Next, suppose that $2^\nu \mid\mid (A_n, R, \Delta)$. When $\nu > 2$, we see that $2 \mid P$ and since Q is odd, we must have $P/2$ odd. Since

$$A_{k+2} \equiv PA_{k+1} - QA_k \pmod 4$$

and $Q \equiv P/2 \equiv 1 \pmod 2$, $2 \mid\mid A_1$ and $2 \mid\mid A_2$, we find by induction on n that $2 \mid\mid A_n$. This is a contradiction to the fact $\nu > 2$. □

Corollary 4.2.1. *If* $(Q, R) = 1$, *then* $(W_n, R, \Delta) \mid 4$.

Proof. Since $W_n = A_nB_n - 3R^n$, we get $(W_n, R) = (A_nB_n, R) = (A_n, R)$ by Lemma 4.1. Hence, $(W_n, R, \Delta) \mid 4$ by the previous theorem. □

To prove the next lemma we first note that since

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

we must have $\Delta \equiv 0, 1 \pmod 4$.

Lemma 4.3. *If* $2 \nmid R$ *and* $2^\alpha \mid\mid (W_n, C_n)$, *then* $\alpha \in \{0, 1\}$, *and if* $2 \mid W_n$, *then* $\tilde{Q}_n = \frac{W_n^2 - \Delta C_n^2}{4}$ *is odd.*

Proof. If $2 \nmid W_n$ we are done. Suppose $2 \mid W_n$. Since $2 \nmid R$ we must have $2 \nmid A_nB_n$, as $A_nB_n = W_n + 3R^n$. So both A_n and B_n are odd and then $2 \mid A_n^2 - 3B_n$.

By Theorem 3.3 we have

$$27\Delta C_n^2 = 4(A_n^2 - 3B_n)^3 - (2A_n^3 - 9W_n)^2.$$

Hence

$$27\Delta C_n^2 \equiv -(2A_n^3 - 9W_n)^2 \pmod 8.$$

Now, since $2A_n^3 - 9W_n \equiv 2 - W_n \pmod 4$, we get

$$27\Delta C_n^2 \equiv -(2 - W_n)^2 \pmod 8.$$

If $2 \mid\mid W_n$, then $8 \mid \Delta C_n^2$ and $\tilde{Q}_n$ is odd. If $4 \mid W_n$, then $27\Delta C_n^2 \equiv -4 \pmod 8$ and $\tilde{Q}_n$ is odd, thus, if $4 \mid \Delta$ then $C_n \equiv 1 \pmod 2$. If $\Delta \equiv 1 \pmod 4$, then $C_n \equiv 2 \pmod 4$.

□

Lemma 4.4. *If $2 \mid R$, $2 \nmid Q$ and $2^\alpha \mid\mid (W_n, C_n)$, then $\alpha \in \{0, 1\}$, and if $2 \mid W_n$, then $\tilde{Q}_n$ is odd.*

Proof. If $2 \nmid W_n$ we are done. If $2 \mid W_n$, then $2 \mid A_n B_n$. Since $2 \nmid Q$ we know $2 \nmid B_n$ and $2 \mid A_n$. We may then observe that $A_n^2 - 3B_n$ is odd and thus

$$\begin{aligned} 27\Delta C_n^2 &\equiv 4 - (2A_n^3 - 9W_n)^2 \pmod 8 \\ &\equiv 4 - (-9W_n)^2 \pmod 8 \\ &\equiv 4 - W_n^2 \pmod 8. \end{aligned}$$

If $2 \mid\mid W_n$, then $8 \mid \Delta C_n^2$ and $\tilde{Q}_n$ is odd. If $4 \mid W_n$, then $27\Delta C_n^2 \equiv 4 \pmod 8$ or $-\Delta C_n^2 \equiv 4 \pmod 8$ which implies C_n is odd or $2 \mid\mid C_n$; in either case $\tilde{Q}_n$ is odd. □

From the above results we have the following theorem.

Theorem 4.5. *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 (2.18).

Lemma 4.6. *If* $(Q, R) = 1$*, then*

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

Proof. If $(W_n, C_n, R) = 1$, we are done. 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 by equation (3.5) $W_n^2 - \Delta C_n^2 = 4S_nT_n = 4(3R^{2n} + R^nA_{3n} + B_{3n}) \Rightarrow p \mid 4B_{3n}$. Also, $B_{3n} = B_n^3 - 3R^nA_nB_n + 3R^{2n}$, so $p \mid 4B_n^3$. Since $(Q, R) = 1$, we have $(B_n, R) = 1$ by Lemma 4.1 but this implies $p \nmid B_n \Rightarrow p = 2$. Indeed, by Lemma 4.4, we must have $(W_n, C_n, R) \mid 2$. □

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

$$C_m \mid C_n, \quad \text{when} \quad m \mid n. \tag{4.1}$$

Note that if $n = ms$, then

$$\begin{aligned} C_n(P, Q, R) &= \frac{(\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)}{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)} = \frac{(\alpha^{ms} - \beta^{ms})(\beta^{ms} - \gamma^{ms})(\gamma^{ms} - \alpha^{ms})}{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)} \\ &= \frac{(\alpha^m - \beta^m)(\beta^m - \gamma^m)(\gamma^m - \alpha^m)}{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)} \cdot \frac{(\alpha^{ms} - \beta^{ms})(\beta^{ms} - \gamma^{ms})(\gamma^{ms} - \alpha^{ms})}{(\alpha^m - \beta^m)(\beta^m - \gamma^m)(\gamma^m - \alpha^m)} \\ &= C_m(P, Q, R) \cdot C_s(A_m, B_m, R^m). \end{aligned}$$

Definition 4.7. *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 2.4 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 4.8. *Let r_1 be the least positive integer for which $p \mid C_{r_1}$. For $i = 1, 2, \ldots, k$ define r_{i+1}, if it exists, to be the least positive integer such that $p \mid C_{r_{i+1}}$, $r_{i+1} > r_i$ and $r_j \nmid r_{i+1}$ for any $j \leq i+1$. We define r_1, r_2, ..., r_k to be the ranks of apparition 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. Here, $C_6 \equiv 0 \pmod{p}$, $C_{10} \equiv 0 \pmod{p}$ and $C_{15} \equiv 0 \pmod{p}$.

Our sequence $\{C_n\}$ also fails to satisfy the generalization of Corollary 2.4.1 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 can, however, reach a relatively close analogue to Carmichael's result seen in Theorem 2.5. To do so we must first derive several preliminary arithmetic results in the next lemmas and theorems.

Lemma 4.9. *If*

$$I_m = \sum \frac{m(-1)^{\lambda_0}(m - \lambda_0 - 1)!}{\lambda_1!\lambda_2!\lambda_3!} \tag{4.2}$$

is summed over all $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}^{\geq 0}$ such that $\lambda_0+\lambda_1+\lambda_2+\lambda_3 = m$, $\lambda_1+2\lambda_2+3\lambda_3 = m$ and $\lambda_1 \not\equiv \lambda_2 \pmod{2}$, then $I_m \equiv m \pmod{2}$.

Proof. Put I'_m equal to the right side of (4.2), where we insist that $\lambda_1 \equiv \lambda_2 \pmod 2$.

By Waring's theorem

$$\alpha^m + \beta^m + \gamma^m = \sum \frac{m(-1)^{\lambda_0}(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} P^{\lambda_1} Q^{\lambda_2} R^{\lambda_3},$$

where the sum is over all λ_i satisfying the constraints in the statement of the lemma except that of $\lambda_1 \not\equiv \lambda_2 \pmod 2$. This is true as $P = \alpha + \beta + \gamma$, $Q = \alpha\beta + \beta\gamma + \gamma\alpha$ and $R = \alpha\beta\gamma$.

Putting $P = Q = R = 1$ we get

$$\alpha^m + \beta^m + \gamma^m = I'_m + I_m$$

so $I'_m + I_m = 1^m + i^m + (-i)^m \equiv 1 \pmod 2$, where $i^2 = -1$. Putting $P = Q = -1$, $R = 1$ we have $\alpha = -1$, $\beta = -1$,$\gamma = 1$, yielding $I'_m - I_m = 2(-1)^m + 1$. It then follows that

$$I_m = \frac{i^m + (-i)^m}{2} - (-1)^m \equiv m \pmod 2.$$

□

Let $\tilde{P}_n = W_n$ and $\tilde{Q}_n = (W_n^2 - \Delta C_n^2)/4$ for the remainder of this section. We will now give a series of results that will be useful in the next chapter.

Theorem 4.10. *If* $2 \mid \tilde{P}_n$ *and* $2 \nmid \tilde{Q}_n$, *then* $\frac{C_{mn}}{C_n} \equiv m \pmod 2$.

Proof. First note that, by equation (2.7), we can derive

$$-\tilde{Q}_n^{\lambda_2} U_{\lambda_1 - \lambda_2} = \tilde{Q}_n^{\lambda_1} U_{\lambda_2 - \lambda_1} \tag{4.3}$$

and if $k \geq 0$, $U_k(\tilde{P}_n, \tilde{Q}_n) \equiv U_k(2,1) \equiv k \pmod 2$. It follows that

$$\tilde{Q}_n^{\lambda_1} U_{\lambda_2 - \lambda_1} \equiv \lambda_2 - \lambda_1 \pmod 2$$

for $\lambda_2 \geq \lambda_1$ and $\lambda_2 < \lambda_1$. Hence by the multiplication formula for C_{mn}, we get

$$\frac{C_{mn}}{C_n} \equiv \sum \frac{m(-1)^{\lambda_0}(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{(\lambda_0+\lambda_3)n} \pmod 2$$

where the sum is as in (3.17) with the extra condition $\lambda_1 \not\equiv \lambda_2 \pmod 2$.

If $2 \mid R$, then each of the terms in the expression for C_{mn}/C_n modulo 2 is even unless $\lambda_0 + \lambda_3 = 0$, $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = m$, $\lambda_1 + 2\lambda_2 + 3\lambda_3 = m$ and $2 \nmid (\lambda_1 + \lambda_2)$. These conditions imply $\lambda_0 = \lambda_3 = 0 \Rightarrow \lambda_2 = 0 \Rightarrow \lambda_1 = m \Rightarrow 2 \nmid m$. In this case

$$\begin{aligned} \frac{C_{mn}}{C_n} &\equiv \frac{m(-1)^{\lambda_0}(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{(\lambda_0+\lambda_3)n} \\ &\equiv 1 \pmod 2. \end{aligned}$$

If $2 \nmid R$, then by Lemma 4.9

$$\frac{C_{mn}}{C_n} \equiv I_m \equiv m \pmod 2.$$

□

Lemma 4.11. *If* $\frac{C_{rn}}{C_n} \equiv 0 \pmod k$ *for all* $n > 0$, *then* $\frac{C_{mn}}{C_n} \equiv 0 \pmod k$ *if* $r \mid m$.

Proof. Let $m = rs$. Then it is easy to see that

$$\frac{C_{mn}}{C_n} = \frac{C_{rsn}}{C_n} = \frac{C_{rsn}}{C_{rn}} . \frac{C_{rn}}{C_n} \equiv 0 \pmod k.$$

□

Theorem 4.12. *If* $2 \nmid R$, $2 \mid \tilde{P}_n$, $2 \mid \tilde{Q}_n$, *then*

$$\begin{aligned} \frac{C_{mn}}{C_n} &\equiv m \pmod 2 \text{ if } 3 \nmid m \\ \frac{C_{mn}}{C_n} &\equiv 0 \pmod 2 \text{ if } 3 \mid m. \end{aligned}$$

Proof. Note that $\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} \equiv 0 \pmod 2$ unless $\lambda_2 = 0$, $\lambda_1 = 1$ or $\lambda_1 = 0$, $\lambda_2 = 1$. We now consider these cases where $\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} \not\equiv 0 \pmod 2$.

It follows that if $m \equiv 1 \pmod 3$ it must be that $\lambda_2 = 0$, $\lambda_1 = 1$, $\lambda_3 = \frac{m-1}{3}$ and $\lambda_0 = 2\frac{m-1}{3}$. So $m - \lambda_0 - 1 = \frac{m-1}{3}$. This implies

$$\frac{C_{nm}}{C_n} \equiv m \frac{\left(\frac{m-1}{3}\right)!}{\left(\frac{m-1}{3}\right)!} \equiv m \pmod 2.$$

Similarly, if $m \equiv -1 \pmod 3$, we can only have $\lambda_2 = 1$, $\lambda_1 = 0$, $\lambda_3 = \frac{m-2}{3}$ and $\lambda_0 = \frac{2m-1}{3}$. Hence $m - \lambda_0 - 1 = \frac{m-2}{3}$, which gives

$$\frac{C_{mn}}{C_n} \equiv m \pmod 2.$$

If $3 \mid m$ we can never have $\lambda_2 = 0$, $\lambda_1 = 1$, or $\lambda_1 = 0$, $\lambda_2 = 1$. Thus,

$$\frac{C_{nm}}{C_n} \equiv 0 \pmod 2.$$

□

Theorem 4.13. *If $2 \nmid R$, $2 \nmid \tilde{P}_n$ and $2 \nmid \tilde{Q}_n$, then*

$$\frac{C_{mn}}{C_n} \equiv 1 \pmod 2 \text{ if } 3 \nmid m$$
$$\frac{C_{mn}}{C_n} \equiv 0 \pmod 2 \text{ if } 3 \mid m.$$

Proof. First note that

$$U_t(\tilde{P}_n, \tilde{Q}_n) \equiv U_t(1,1) \equiv \begin{cases} 0 & \text{if } 3 \mid t \\ 1 & \text{if } 3 \nmid t \end{cases} \pmod 2.$$

Hence

$$\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} \equiv \begin{cases} 0 & \text{if } 3 \mid \lambda_1 - \lambda_2 \\ 1 & \text{if } 3 \nmid \lambda_1 - \lambda_2 \end{cases} \pmod 2.$$

Since $\lambda_1 + 2\lambda_2 + 3\lambda_3 = m$, we see that if $\lambda_1 \equiv \lambda_2 \pmod 3$, then $3 \mid m$. It follows that if $3 \nmid m$, we know $\lambda_1 \not\equiv \lambda_2 \pmod 3$ and we get

$$\frac{C_{mn}}{C_n} \equiv \sum \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} = I_m + I'_m \equiv 1 \pmod 2.$$

We note that $\frac{C_{3n}}{C_n} = (\Delta C_n^2 + 3W_n^2)/4 = \tilde{P}_n^2 - \tilde{Q}_n \equiv 0 \pmod 2$, thus in the case where $3 \mid m$, it follows from Lemma 4.11 that $\frac{C_{mn}}{C_n} \equiv 0 \pmod 2$. □

Theorem 4.14. *If $2 \nmid R$, $2 \nmid \tilde{P}_n$ and $2 \mid \tilde{Q}_n$, then*

$$\frac{C_{mn}}{C_n} \equiv 1 \pmod 2 \text{ if } 7 \nmid m$$
$$\frac{C_{mn}}{C_n} \equiv 0 \pmod 2 \text{ if } 7 \mid m.$$

Proof. First, we use the fact that

$$U_t(\tilde{P}_n, \tilde{Q}_n) \equiv U_t(1,0) \pmod 2.$$

This implies

$$U_t(\tilde{P}_n, \tilde{Q}_n) \equiv 1 \pmod 2 \text{ if } t > 0.$$

Now, $\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} \equiv 0 \pmod 2$ if $\lambda_1 \geq \lambda_2 > 0$ or $\lambda_2 \geq \lambda_1 > 0$. Thus, if $\lambda_1 = 0$, $\lambda_2 \geq 1$ or $\lambda_2 = 0$, $\lambda_1 \geq 1$, then

$$\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} \equiv 1 \pmod 2$$

as $\tilde{Q}_n^t U_{-t} = -U_t$.

It follows that

$$\frac{C_{mn}}{C_n} \equiv \sum_{\substack{\lambda_0+\lambda_1+\lambda_3=m \\ \lambda_1+3\lambda_3=m}} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_3!} + \sum_{\substack{\lambda_0+\lambda_2+\lambda_3=m \\ 2\lambda_2+3\lambda_3=m}} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_2!\lambda_3!} \pmod 2.$$

Now let us restrict ourselves to the case where $P=1$, $Q=0$, $R=1$ and α, β, γ are the zeros of $X^3 - PX^2 + QX - R$. Then

$$A_m = \alpha^m + \beta^m + \gamma^m = \sum_{\substack{\lambda_0+\lambda_1+\lambda_3=m \\ \lambda_1+3\lambda_3=m}} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_3!}.$$

Also let $P'=0$, $Q'=1$, $R'=1$ and α', β', γ' be the zeros of $X^3 - P'X^2 + Q'X - R'$, then

$$A'_m = \alpha'^m + \beta'^m + \gamma'^m = \sum_{\substack{\lambda_0+\lambda_2+\lambda_3=m \\ 2\lambda_2+3\lambda_3=m}} \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_2!\lambda_3!}.$$

Clearly, the above two identities follow from Waring's theorem.

Now it is clear that $A'_0 = 3$, $A'_1 = P' = 0$, $A'_2 = P'^2 - 2Q' = -2$ and

$$A'_{n+3} = P'A'_{n+2} - Q'A'_{n+1} + R'A'_n \equiv A'_{n+1} + A'_n \pmod 2.$$

Thus,

$$\begin{aligned} A'_m &\equiv 1 \pmod 2 \text{ if } m \equiv 0,3,5,6 \pmod 7 \\ A'_m &\equiv 0 \pmod 2 \text{ if } m \equiv 1,2,4 \pmod 7. \end{aligned}$$

Similarly, one can show that

$$\begin{aligned} A_m &\equiv 1 \pmod 2 \text{ if } m \equiv 0,1,2,4 \pmod 7 \\ A_m &\equiv 0 \pmod 2 \text{ if } m \equiv 3,5,6 \pmod 7. \end{aligned}$$

Hence

$$\begin{aligned} A_m + A'_m &\equiv 1 \pmod 2 \text{ if } 7 \nmid m \\ A_m + A'_m &\equiv 0 \pmod 2 \text{ if } 7 \mid m. \end{aligned}$$

Since $\frac{C_{mn}}{C_n} \equiv A_m + A'_m \pmod 2$, we are done. □

We now assume that $(Q, R) = 1$, and we recall from Theorem 4.5 that if $2 \mid \tilde{P}_n$, then $2 \nmid \tilde{Q}_n$. Putting $n = 1$, from these results, we now know that

$$C_m \equiv m \pmod 2$$

when $2 \mid \tilde{P}_1$, $2 \nmid \tilde{Q}_1$. Put $r = 2$ in this case.

If $2 \nmid R$, $2 \nmid \tilde{P}_1$, $2 \nmid \tilde{Q}_1$, put $r = 3$ and note that

$$\begin{aligned} C_m &\equiv 1 \pmod 2 \quad \text{if} \quad 3 \nmid m, \\ C_m &\equiv 0 \pmod 2 \quad \text{if} \quad 3 \mid m. \end{aligned}$$

If $2 \nmid R$, $2 \nmid \tilde{P}_1$, $2 \mid \tilde{Q}_1$, put $r = 7$ and note that

$$C_m \equiv 1 \pmod 2 \quad \text{if} \quad 7 \nmid m,$$
$$C_m \equiv 0 \pmod 2 \quad \text{if} \quad 7 \mid m.$$

There remains the case of $2 \nmid \tilde{P}_1$ and $2 \mid R$. We have $2 \nmid Q$; thus, by Corollary 3.14.2, we get $2 \nmid \tilde{Q}_1$ and

$$C_m \equiv U_m(1,1) \pmod 2.$$

In this case, we put $r = 3$ and we have

$$C_m \equiv 1 \pmod 2 \quad \text{if} \quad 3 \nmid m,$$
$$C_m \equiv 0 \pmod 2 \quad \text{if} \quad 3 \mid m.$$

Hence, we have proved the following theorem.

Theorem 4.15. *If $(Q, R) = 1$, there always exists a minimal $r > 1$ such that $2 \mid C_r$. Furthermore, if $2 \mid C_n$, then $r \mid n$.*

Lemma 4.16. *If m, $n \geq 1$, then*

$$\frac{C_{mn}}{C_n} \equiv 0 \pmod{(\tilde{P}_n, \tilde{Q}_n)} \text{ if } 3 \mid m$$
$$\frac{C_{mn}}{C_n} \equiv mR^{(m-1)n} \pmod{(\tilde{P}_n, \tilde{Q}_n)} \text{ if } 3 \nmid m.$$

Proof. Recall for $U_k(\tilde{P}_n, \tilde{Q}_n)$, $U_{-k} = -U_k/\tilde{Q}_n^k$. By (4.3) we see that if $\lambda_1 \geq \lambda_2$, then

$$\begin{aligned}
\tilde{Q}_n^{\lambda_2} U_{\lambda_1 - \lambda_2} &\equiv 0 \pmod{\tilde{Q}_n} \text{ if } \lambda_2 \geq 1, \\
\tilde{Q}_n^{\lambda_2} U_{\lambda_1 - \lambda_2} &\equiv U_{\lambda_1} \equiv \tilde{P}_n^{\lambda_1 - 1} \pmod{\tilde{Q}_n} \text{ if } \lambda_2 = 0 \neq \lambda_1, \\
\tilde{Q}_n^{\lambda_2} U_{\lambda_1 - \lambda_2} &\equiv 0 \pmod{\tilde{Q}_n} \text{ if } \lambda_1 = \lambda_2.
\end{aligned}$$

For $\lambda_2 \geq \lambda_1$, we have the following results:

$$\begin{aligned}
-\tilde{Q}_n^{\lambda_1} U_{\lambda_2-\lambda_1} &\equiv 0 \pmod{\tilde{Q}_n} \text{ if } \lambda_1 \geq 1, \\
-\tilde{Q}_n^{\lambda_1} U_{\lambda_2-\lambda_1} &\equiv -U_{\lambda_2} \equiv -\tilde{P}_n^{\lambda_2-1} \pmod{\tilde{Q}_n} \text{ if } \lambda_1 = 0 \neq \lambda_2, \\
-\tilde{Q}_n^{\lambda_1} U_{\lambda_2-\lambda_1} &\equiv 0 \pmod{\tilde{Q}_n} \text{ if } \lambda_1 = \lambda_2.
\end{aligned}$$

Thus $\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} \equiv 0 \pmod{\tilde{Q}_n}$ unless $\lambda_1 \geq 1$, $\lambda_2 = 0$ or $\lambda_1 = 0$, $\lambda_2 \geq 1$. But since $(\tilde{P}_n, \tilde{Q}_n)$ will divide $\tilde{P}_n$, we get $\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} \equiv 0 \pmod{(\tilde{P}_n, \tilde{Q}_n)}$ unless $\lambda_1 = 1$, $\lambda_2 = 0$ or $\lambda_1 = 0$, $\lambda_2 = 1$.

If $3 \mid m$, then $3 \mid \lambda_1 + 2\lambda_2$ and neither $\lambda_1 = 1$, $\lambda_2 = 0$ nor $\lambda_1 = 0$, $\lambda_2 = 1$ can occur. Thus, from Theorem 3.14 we can conclude that

$$\frac{C_{mn}}{C_n} \equiv 0 \pmod{(\tilde{P}_n, \tilde{Q}_n)} \quad \text{if} \quad 3 \mid m.$$

If $3 \nmid m$, then either $m \equiv 1 \pmod 3$ or $m \equiv 2 \pmod 3$. If $m \equiv 1 \pmod 3$, then we must have $\lambda_1 = 1$, $\lambda_2 = 0$, in which case $\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} = 1$, $\lambda_3 = \frac{m-1}{3}$, $\lambda_3 = m - \lambda_0 - 1$, and $\lambda_0 = 2\frac{m-1}{3}$. Applying the above to Theorem 3.14 yields

$$\frac{C_{mn}}{C_n} \equiv mR^{(m-1)n} \pmod{(\tilde{P}_n, \tilde{Q}_n)} \quad \text{if} \quad m \equiv 1 \pmod 3.$$

Similarly, if $m \equiv 2 \pmod 3$, then it must be that $\lambda_1 = 0$, $\lambda_2 = 1$. Then we can see $-\tilde{Q}_n^{\lambda_1} U_{\lambda_2-\lambda_1} = \tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2} = \tilde{Q}_n U_{-1} = -U_1 = -1$, $\lambda_3 = \frac{m-2}{3}$, $\lambda_0 = \frac{2m-1}{3}$ which is odd. Again use Theorem 3.14 to get

$$\frac{C_{mn}}{C_n} \equiv mR^{(m-1)n} \pmod{(\tilde{P}_n, \tilde{Q}_n)} \quad \text{if} \quad m \equiv 2 \pmod 3.$$

Which completes the proof. □

Corollary 4.16.1. *If $3 \nmid m$, then*

$$(C_{mn}/C_n, \tilde{P}_n, \tilde{Q}_n) \mid mR^{n(m-1)}.$$

Proof. This follows immediately from Lemma 4.16. □

Theorem 4.17. *If* $2 \nmid R$ *or if* $2 \mid R$ *and* $2 \nmid Q$*, then*

$$(C_{mn}/C_n, W_n, C_n) \mid mR^{n(m-1)} \text{ when } 3 \nmid m.$$

Proof. We have by Corollary 4.16.1 that if $3 \nmid m$, then

$$(C_{mn}/C_n, \tilde{P}_n, \tilde{Q}_n) \mid mR^{n(m-1)} \Rightarrow (C_{mn}/C_n, W_n, (W_n^2 - \Delta C_n^2)/4) \mid mR^{n(m-1)}.$$

We divide our proof into 2 cases.

Case 1: $2 \nmid W_n$. In this case

$$(4C_{mn}/C_n, 4W_n, W_n^2 - \Delta C_n^2) \mid 4mR^{n(m-1)} \Rightarrow (C_{mn}/C_n, W_n, C_n) \mid 4mR^{n(m-1)}.$$

But since W_n is odd $(C_{mn}/C_n, W_n, C_n) \mid mR^{n(m-1)}$.

Case 2: $2 \mid W_n$. In this case we have $2 \mid \tilde{P}_n$ and $\tilde{Q}_n$ is odd, so by Theorem 4.10

$$\frac{C_{mn}}{C_n} \equiv m \pmod 2.$$

Also, we know by Theorem 4.5 that if $2^s \mid\mid (W_n, C_n)$ then $s \in \{0, 1\}$.

Since $(C_{mn}/C_n, W_n, C_n) \mid 4mR^{n(m-1)}$ we see that $(C_{mn}/C_n, W_n, C_n) \mid mR^{n(m-1)}$ when m is odd. Otherwise, if m is even and $2^s \mid\mid (C_{mn}/C_n, W_n, C_n)$, then $s \in \{0, 1\}$. If $s = 0$, then $(C_{mn}/C_n, W_n, C_n) | mR^{n(m-1)}$. If $s = 1$, then $2 \mid\mid (C_{mn}/C_n, W_n, C_n)$, which implies $(C_{mn}/C_n, W_n, C_n) \mid mR^{n(m-1)}$. □

We have been working towards the following corollary which is somewhat analogous to Carmichael's result seen in Theorem 2.5. We will derive a closer analogue in Chapter 5.

Corollary 4.17.1. *If* $(Q, R) = 1$*, then*

$$(C_{mn}/C_n, W_n, C_n) \mid m \text{ when } 3 \nmid m.$$

Proof. If $(W_n, C_n, R) = 1$, we are done. Let p be any prime such that $p \mid (W_n, C_n, R)$. By Lemma 4.6 we can only have $p = 2$. Since $2 \mid W_n$ we have $\tilde{Q}_n$ odd and then by Theorem 4.10 we have

$$\frac{C_{mn}}{C_n} \equiv m \pmod 2.$$

Now if $2 \nmid m$, then

$$(C_{mn}/C_n, W_n, C_n, R) = 1 \Rightarrow (C_{mn}/C_n, W_n, C_n) \mid m.$$

If $2 \mid m$, then

$$(C_{mn}/C_n, W_n, C_n, R^{n(m-1)}) = 2 \Rightarrow (C_{mn}/2C_n, W_n/2, C_n/2, R^{n(m-1)}/2) = 1.$$

We have then

$$(C_{mn}/2C_n, W_n/2, C_n/2) \mid mR^{n(m-1)}/2 \Rightarrow (C_{mn}/2C_n, W_n/2, C_n/2) \mid m$$

$$\Rightarrow (C_{mn}/C_n, W_n, C_n) \mid 2m.$$

But $2 \mid\mid (C_{mn}/C_n, W_n, C_n)$ and $2 \mid m \Rightarrow (C_{mn}/C_n, W_n, C_n) \mid m$. □

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

4.2 Preliminary Results for the Law of Repetition for $\{C_n\}$

We will now require some elementary results in algebraic number theory to develop the proof of the following theorem. This result will be of some importance in establishing a law of repetition for $\{C_n\}$.

Theorem 4.18. *If p is a prime and $p \nmid 6R\Delta$, $p \mid C_n$ and $p \mid W_n - 6R^n$, then $p^3 \mid C_n$ and $p^2 \mid W_n - 6R^n$.*

Proof. Let α, β, γ be the distinct ($p \nmid \Delta$) zeros of $x^3 - Px^2 + Qx - R$ and put $\mathbb{L} = \mathbb{Q}(\alpha)$. If we put $\mathbb{K} = \mathbb{Q}(\alpha, \beta)$, then $\mathbb{K}$ is the normal closure of $\mathbb{L}$ and is, of course, Galois. Put $\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$, $\lambda_1 = \alpha^n - \beta^n$, $\lambda_2 = \beta^n - \gamma^n$ and $\lambda_3 = \gamma^n - \alpha^n$. Note $\lambda_1 + \lambda_2 + \lambda_3 = 0$.

Since $\delta C_n = \lambda_1\lambda_2\lambda_3$, we note that if $\mathfrak{p}$ is prime ideal divisor of (p) in $\mathbb{K}$, then $\mathfrak{p} \mid (\lambda_1\lambda_2\lambda_3)$. We also note that the discriminant of $\mathbb{L}$ must divide Δ. It follows (see for example, Theorem 86 of [Hil98]), that since $p \nmid \Delta$, then p cannot divide the discriminant of $\mathbb{K}$. Thus, in $\mathbb{K}$ we must have

$$(p) = \prod_{i=1}^{k} \mathfrak{p}_i,$$

where the prime ideals $\mathfrak{p}_i$ $(i = 1, 2, \ldots, k)$ are all distinct, that is $(\mathfrak{p}_i, \mathfrak{p}_j) = \mathfrak{O}$, the maximal order of $\mathbb{K}$, for $i \neq j$. Since $\mathfrak{p} \mid (\lambda_1\lambda_2\lambda_3)$, we must have $\mathfrak{p} \mid (\lambda_1)$ or $\mathfrak{p} \mid (\lambda_2)$ or $\mathfrak{p} \mid (\lambda_3)$. Without loss of generality, suppose $\mathfrak{p} \mid (\lambda_1)$.

Since

$$W_n - 6R^n = 2\beta^n(\alpha^n - \gamma^n)^2 - (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\alpha^n + \gamma^n)$$

and $p \mid W_n - 6R^n$, we have

$$2\beta^n(\alpha^n - \gamma^n)^2 \equiv (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\alpha^n + \gamma^n) \equiv 0 \pmod{\mathfrak{p}}.$$

Since $(p, 2R) = 1$ and $R = \alpha\beta\gamma$, we must have $\mathfrak{p} \nmid \beta$ and hence $\alpha^n \equiv \gamma^n \pmod{\mathfrak{p}} \Rightarrow \mathfrak{p} \mid (\lambda_3)$. Also since $\lambda_2 = -\lambda_1 - \lambda_3$ and $(\lambda_1) \equiv (\lambda_3) \equiv 0 \pmod{\mathfrak{p}}$ we must have $(\lambda_2) \equiv 0 \pmod{\mathfrak{p}}$. Hence $\mathfrak{p}^3 \mid (\lambda_1\lambda_2\lambda_3)$. Since $((p), (\delta)) = \mathfrak{O}$, we get $\mathfrak{p}^3 \mid ((\lambda_1\lambda_2\lambda_3)/\delta)$.

Since $\mathfrak{p}_i^3 \mid ((\lambda_1\lambda_2\lambda_3)/\delta)$ for $i = 1, 2, \ldots, k$ and the $\mathfrak{p}_i$ for $i = 1, 2, \ldots, k$ are distinct prime ideals, we must have

$$\prod_{i=1}^{k} \mathfrak{p}_i^3 \mid ((\lambda_1\lambda_2\lambda_3)/\delta).$$

Thus $(p^3) \mid (C_n) \Rightarrow p^3 \mid C_n$. Note that we also have $p^2 \mid W_n - 6R^n$. □

Suppose again that the prime $p \nmid 6\Delta R$ and that $p^\mu \mid\mid C_n$, $p^\nu \mid\mid W_n - 6R^n$, where $\mu, \nu \geq 1$. Let $\mathfrak{p}$ be any of the distinct ideals which lie over (p) in $\mathbb{K}$. Since

$$\mathfrak{p}^\mu \mid\mid (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n),$$

we may assume without loss of generality that

$$\mathfrak{p}^{\mu_1} \mid\mid \alpha^n - \beta^n, \quad \mathfrak{p}^{\mu_2} \mid\mid \beta^n - \gamma^n, \quad \mathfrak{p}^{\mu_3} \mid\mid \gamma^n - \alpha^n,$$

where $\mu_1 + \mu_2 + \mu_3 = \mu$ and $\mu_1 \geq \mu_2 \geq \mu_3$. Since

$$\gamma^n - \alpha^n = -(\beta^n - \gamma^n) - (\alpha^n - \beta^n),$$

we see that $\mathfrak{p}^{\mu_2} \mid \gamma^n - \alpha^n$ and $\mu_2 \leq \mu_3$. Hence $\mu_2 = \mu_3$. If $\mu_1 > \mu_2$, then since

$$W_n - 6R^n = 2\beta^n(\alpha^n - \gamma^n)^2 - (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\alpha^n + \gamma^n)$$

and $\mu_1 + \mu_2 > 2\mu_2$, we must have $\mathfrak{p}^{2\mu_2} \mid\mid W_n - 6R^n$ and $2\mu_2 < \mu$. Thus, $\nu = 2\mu_2 < \mu$. If $\mu_1 = \mu_2$, then $3 \mid \mu$ and $\mu_1 = \mu_2 = \mu_3 = \mu/3$. This seems to suggest that the case of $\nu > \mu$ would occur less frequently than the case of $\nu \leq \mu$.

Put $D_n = (W_n - 6R^n, C_n)$. Since $(W_n, C_n, R) \mid 2$ by Lemma 4.6, we see that if $p \neq 2$ and $p \mid D_n$, then $p \nmid R$. Further results on D_n will be developed in the following chapter. We also have the following theorem for the case where $p = 2$.

Theorem 4.19. *If* $2 \nmid R\Delta$ *and* $16 \mid C_n$, *then* $8 \mid W_n - 6R^n$.

Proof. We note that if $2 \nmid R$ and $4 \mid C_n$, then $2 \mid\mid W_n$ by Theorem 4.5. Thus $W_n - 6R^n \equiv 0 \pmod 4$. Now since $2 \nmid \Delta$, we have (2) is the product of distinct prime ideals in $\mathbb{K}$. Let $\mathfrak{p}$ be any one of these prime ideals. Since $16 \mid (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)$, we must have $\mathfrak{p}^4 \mid (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n)$. Without loss of generality, let $\mathfrak{p}^{\mu_1} \mid\mid (\alpha^n - \beta^n)$, $\mathfrak{p}^{\mu_2} \mid\mid (\beta^n - \gamma^n)$ and $\mathfrak{p}^{\mu_3} \mid\mid (\gamma^n - \alpha^n)$, where $\mu_1 \geq \mu_2 \geq \mu_3$. We must have $\mu_1 + \mu_2 + \mu_3 = 4 \Rightarrow \mu_1 \geq 2$ and $\mu_2 \geq 1$.

Since $\mathfrak{p}^2 \mid W_n - 6R^n$, we get

$$\mathfrak{p}^2 \mid 2\beta^n(\alpha^n - \gamma^n)^2 - (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\alpha^n + \gamma^n).$$

Since $\mathfrak{p}^3 \mid (\alpha^n - \beta^n)(\beta^n - \gamma^n)$, we get $\mathfrak{p}^2 \mid 2\beta^n(\alpha^n - \gamma^n)^2 \Rightarrow \mathfrak{p} \mid (\alpha^n - \gamma^n)^2 \Rightarrow \mathfrak{p} \mid \alpha^n - \gamma^n \Rightarrow \mathfrak{p}^3 \mid W_n - 6R^n$. It follows that $8 \mid W_n - 6R^n$. □

4.3 The Polynomial $K_m(x)$

We now introduce the polynomials $H_m(X, Y)$ and $K_m(X)$. We will develop some properties of these polynomials which will help us to produce the law of repetition for $\{C_n\}$. Put

$$H_m(X, Y) = \sum \frac{(-1)^{\lambda_0} m(m - \lambda_0 - 1)!}{\lambda_1!\lambda_2!\lambda_3!} X^{\lambda_1 - \lambda_2} Y^{2\lambda_2}$$

and

$$K_m(X) = \sum \frac{(-1)^{\lambda_0} m(m - \lambda_0 - 1)!(\lambda_1 - \lambda_2)}{\lambda_1!\lambda_2!\lambda_3!} X^{\lambda_1 + \lambda_2 - 1}. \tag{4.4}$$

As before, the sums are extended over the values $\lambda_i \in \mathbb{Z}$ such that

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

Note that

$$K_m(X) = \frac{\partial H_m(X,Y)}{\partial X}\Big|_{Y=X}.$$

Consider

$$F_{X,Y}(Z) = Z^3 - XZ^2 + (Y^2/X)Z - 1$$

and let $\alpha_1(X,Y)$, $\alpha_2(X,Y)$, $\alpha_3(X,Y)$ be the three (not necessarily distinct) zeros of $F_{X,Y}(Z)$. By Waring's theorem

$$H_m(X,Y) = \alpha_1(X,Y)^m + \alpha_2(X,Y)^m + \alpha_3(X,Y)^m.$$

Hence

$$\begin{aligned}\frac{\partial H_m(X,Y)}{\partial X} &= m\left(\alpha_1(X,Y)^{m-1}\frac{\partial \alpha_1(X,Y)}{\partial X} + \alpha_2(X,Y)^{m-1}\frac{\partial \alpha_2(X,Y)}{\partial X}\right. \\ &\qquad \left. +\alpha_3(X,Y)^{m-1}\frac{\partial \alpha_3(X,Y)}{\partial X}\right).\end{aligned}$$

For convenience we will now write α_1, α_2 and α_3, to denote $\alpha_1(X,Y)$, $\alpha_2(X,Y)$ and $\alpha_3(X,Y)$, respectively. One can easily see then,

$$\alpha_1 + \alpha_2 + \alpha_3 = X, \quad \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = Y^2/X \quad \text{and} \quad \alpha_1\alpha_2\alpha_3 = 1.$$

Following Lagrange, we put

$$\begin{aligned}\theta_1(X,Y) &= \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3, \\ \theta_2(X,Y) &= \alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3,\end{aligned}$$

where ζ is a primitive cube root of unity ($\zeta^2 + \zeta + 1 = 0$). Then

$$\begin{aligned}
\alpha_1 &= \frac{1}{3}\left(X + \theta_1 + \theta_2\right), \\
\alpha_2 &= \frac{1}{3}\left(X + \zeta^2\theta_1 + \zeta\theta_2\right), \\
\alpha_3 &= \frac{1}{3}\left(X + \zeta\theta_1 + \zeta^2\theta_2\right).
\end{aligned}$$

Further, one can easily show

$$\theta_1\theta_2 = X^2 - 3Y^2/X \quad \text{and} \quad \theta_1^3 + \theta_2^3 = 2X^3 - 9Y^2 + 27.$$

With these two identities we can show

$$\begin{aligned}
\theta_1^3(X,Y) &= \frac{2X^3 - 9Y^2 + 27 + \sqrt{\Delta(X,Y)}}{2} \quad \text{and} \\
\theta_2^3(X,Y) &= \frac{2X^3 - 9Y^2 + 27 - \sqrt{\Delta(X,Y)}}{2},
\end{aligned}$$

where

$$\begin{aligned}
\Delta(X,Y) &= (2X^3 - 9Y^2 + 27)^2 - 4(X^2 - 3Y^2/X)^3 \\
&= -27(Y^4 - 4Y^6/X^3 - 4X^3 + 18Y^2 - 27).
\end{aligned}$$

Note that

$$\Delta(X,Y)\Big|_{Y=X} = -27\left(X^4 - 8X^3 + 18X^2 - 27\right) = -27\left(X - 3\right)^2\left(X^2 - 2X - 3\right).$$

Put

$$D(X) = X^2 - 2X - 3 = (X - 3)(X + 1).$$

Now, observe

$$\frac{\partial\Delta(X,Y)}{\partial X} = -27(-12X^2 + 12Y^6/X^4) \Rightarrow \frac{\partial\Delta(X,Y)}{\partial X}\Big|_{Y=X} = 0.$$

It is easy to see that

$$\frac{\partial\theta_1(X,Y)}{\partial X} = \frac{1}{3}\theta_1^{-2}\left(6X^2 + \frac{1}{2}\Delta^{-1/2}(X,Y)\frac{\partial\Delta(X,Y)}{\partial X}\right)/2.$$

Thus

$$\frac{\partial\theta_1(X,Y)}{\partial X}\Big|_{Y=X} = \theta_1^{-2}(X,X)X^2.$$

Similarly

$$\frac{\partial\theta_2(X,Y)}{\partial X}\Big|_{Y=X} = \theta_2^{-2}(X,X)X^2.$$

Since

$$\theta_1(X,X)\theta_2(X,X) = X^2 - 3X,$$

we get

$$\theta_1^{-1}(X,X) = \frac{\theta_2(X,X)}{X^2-3X} \quad \text{and} \quad \theta_2^{-1}(X,X) = \frac{\theta_1(X,X)}{X^2-3X}.$$

So we then have

$$\frac{\partial\theta_1(X,Y)}{\partial X}\Big|_{Y=X} = \frac{\theta_2^2(X,X)}{(X-3)^2} \quad \text{and} \quad \frac{\partial\theta_2(X,Y)}{\partial X}\Big|_{Y=X} = \frac{\theta_1^2(X,X)}{(X-3)^2}.$$

Now

$$\begin{aligned}\theta_1(X,X) &= \alpha_1(X,X) + \zeta\alpha_2(X,X) + \zeta^2\alpha_3(X,X) \quad \text{and}\\ F_{X,X}(Z) &= Z^3 - XZ^2 + XZ - 1.\end{aligned}$$

Hence, we may put

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

We then have

$$\begin{aligned}\theta_1(X,X) &= \frac{3-X+(\zeta-\zeta^2)\sqrt{D(X)}}{2},\\ \theta_2(X,X) &= \frac{3-X-(\zeta-\zeta^2)\sqrt{D(X)}}{2}.\end{aligned}$$

Upon squaring and using the fact $(\zeta - \zeta^2)^2 = -3$, we get

$$\begin{aligned}
\theta_1^2(X,X) &= (X-3)\left[\frac{-X-3-(\zeta-\zeta^2)\sqrt{D(X)}}{2}\right], \\
\theta_2^2(X,X) &= (X-3)\left[\frac{-X-3+(\zeta-\zeta^2)\sqrt{D(X)}}{2}\right].
\end{aligned}$$

Hence

$$\begin{aligned}
\frac{\partial\theta_1(X,Y)}{\partial X}\Big|_{Y=X} &= \frac{-X-3+(\zeta-\zeta^2)\sqrt{D(X)}}{2(X-3)}, \\
\frac{\partial\theta_2(X,Y)}{\partial X}\Big|_{Y=X} &= \frac{-X-3-(\zeta-\zeta^2)\sqrt{D(X)}}{2(X-3)}.
\end{aligned}$$

Now

$$\begin{aligned}
\frac{\partial\alpha_1(X,Y)}{\partial X}\Big|_{Y=X} &= \frac{1}{3}\left(1+\frac{\partial\theta_1(X,Y)}{\partial X}+\frac{\partial\theta_2(X,Y)}{\partial X}\right)\Big|_{Y=X} \\
&= \frac{1}{3}\left(1+\frac{-X-3+(\zeta-\zeta^2)\sqrt{D(X)}}{2(X-3)}\right. \\
&\qquad\left.+\frac{-X-3-(\zeta-\zeta^2)\sqrt{D(X)}}{2(X-3)}\right) \\
&= \frac{1}{3}\left(1-\frac{X+3}{X-3}\right) = \frac{-2}{X-3}.
\end{aligned}$$

Also,

$$\begin{aligned}
\frac{\partial\alpha_2(X,Y)}{\partial X}\Big|_{Y=X} &= \frac{1}{3}\left(1+\zeta^2\frac{\partial\theta_1(X,Y)}{\partial X}+\zeta\frac{\partial\theta_2(X,Y)}{\partial X}\right)\Big|_{Y=X} \\
&= \frac{1}{3}\left(1+\frac{X+3+(2-\zeta-\zeta^2)\sqrt{D(X)}}{2(X-3)}\right) \\
&= \frac{X-1+\sqrt{D(X)}}{2(X-3)} = \frac{\alpha_2(X,X)}{X-3}, \\
\frac{\partial\alpha_3(X,Y)}{\partial X}\Big|_{Y=X} &= \frac{1}{3}\left(1+\frac{X+3-(2-\zeta-\zeta^2)\sqrt{D(X)}}{2(X-3)}\right) = \frac{\alpha_3(X,X)}{X-3}.
\end{aligned}$$

It follows that

$$\begin{aligned} K_m(X) &= \frac{\partial H_m(X,Y)}{\partial X}\Big|_{Y=X} \\ &= m\alpha_1^{m-1}(X,X)\left(\frac{-2}{X-3}\right) + m\alpha_2^{m-1}(X,X)\left(\frac{\alpha_2(X,X)}{X-3}\right) \\ &\qquad + m\alpha_3^{m-1}(X,X)\left(\frac{\alpha_3(X,X)}{X-3}\right) \\ &= \frac{m}{X-3}\left[-2+\alpha_2(X,X)^m+\alpha_3(X,X)^m\right]. \end{aligned}$$

We then get the identity

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

If m is odd, then using identity (4.2.44) from [Wil98] gives

$$\begin{aligned} V_m(X-1,1) &= \alpha_2(X,X)^m + \alpha_3(X,X)^m && (4.5) \\ &= (X-1)\sum_{j=0}^{(m-1)/2}\binom{(m-1)/2+j}{(m-1)/2-j}D^j(X). && (4.6) \end{aligned}$$

In this case

$$K_m(X) = m\left[1+\sum_{j=1}^{(m-1)/2}\binom{(m-1)/2+j}{(m-1)/2-j}(X-1)(X+1)^j(X-3)^{j-1}\right].$$

If m is even, then identity (4.2.42) from [Wil98] yields

$$\begin{aligned} V_m(X-1,1) = \alpha_2^m(X,X)+\alpha_3^m(X,X) &= \sum_{j=0}^{m/2}\frac{m}{m/2-j}\binom{m/2+j}{m/2-j}D^j(X) && (4.7) \\ &= 2+\sum_{j=1}^{m/2}\frac{m}{m/2-j}\binom{m/2+j}{m/2-j}D^j(X) && (4.8) \end{aligned}$$

In this case

$$K_m(X) = m\sum_{j=1}^{m/2}\frac{m}{m/2-j}\binom{m/2+j-1}{m/2-j-1}(X+1)^j(X-3)^{j-1}.$$

Theorem 4.20. *Let $X \in \mathbb{Z}$ and p be a prime such that $p > 3$. If $p \nmid X - 3$, then*

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

If $p \mid X - 3$, then

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

Proof. From the top of page 100 we have

$$(X-3)K_p(X) = p(-2 + \alpha_2^p(X,X) + \alpha_3^p(X,X)).$$

Since $\alpha_2\alpha_3 = 1$ and $\alpha_2 + \alpha_3 = X - 1$, we have

$$\alpha_2^p(X,X) + \alpha_3^p(X,X) = V_p(X-1,1) \equiv X - 1 \pmod{p}.$$

Thus $pV_p(X-1,1) \equiv p(X-1) \pmod{p^2}$ and so we have

$$(X-3)K_p(X) \equiv p(X-3) \pmod{p^2} \Rightarrow K_p(X) \equiv p \pmod{p^2}$$

when $p \nmid X - 3$.

Now suppose that $p \mid X - 3$. We know that

$$K_p(X) = p\left[1 + \sum_{j=1}^{(p-1)/2} \binom{(p-1)/2 + j}{(p-1)/2 - j}(X-1)(X+1)^j(X-3)^{j-1}\right].$$

Hence, if $p \geq 7$,

$$\begin{aligned} K_p(X) \equiv\ & p\left[1 + \binom{(p+1)/2}{2}(X^2-1) + \binom{(p+3)/2}{4}(X-3)(X+1)^2(X-1)\right. \\ & \left. + \binom{(p+5)/2}{6}(X-3)^2(X+1)^3(X-1)\right] \pmod{p^4}. \end{aligned}$$

Next note that

$$\begin{aligned} 6\binom{(p+1)/2}{2} + 32\binom{(p+3)/2}{4} &= 6\frac{(p^2-1)}{8} + \frac{(p^2-9)(p^2-1)}{12} \\ &= p^2\left(\frac{p^2-1}{8}\right) \equiv 0 \pmod{p^2}. \end{aligned}$$

Also,

$$\begin{aligned}
&\binom{(p+1)/2}{2} + 32\binom{(p+3)/2}{4} + 128\binom{(p+5)/2}{6} \\
&= \frac{p^2-1}{8} + \frac{(p^2-9)(p^2-1)}{12} + \frac{(p^2-25)(p^2-9)(p^2-1)}{360} \\
&= \left(\frac{p^2-1}{8}\right)\left(1 + \frac{2(p^2-9)}{3} + \frac{(p^2-25)(p^2-9)}{45}\right) \\
&= \left(\frac{p^2-1}{8}\right)\left(\frac{p^4-4p^2}{45}\right) = \frac{p^2(p^2-1)(p^2-4)}{360} \equiv 0 \pmod{p^2}.
\end{aligned}$$

Since $p \neq 3$, by using

$$X^2 - 1 = (X-3)^2 + 6(X-3) + 8,$$

$$(X+1)^2(X-1) = (X-3)^3 + 10(X-3)^2 + 32(X-3) + 32,$$

$$(X+1)^3(X-1) = (X-3)^4 + 14(X-3)^3 + 72(X-3)^2 + 160(X-3) + 128,$$

we can rewrite $K_p(X) \pmod{p^4}$ as follows

$$\begin{aligned}
K_p(X) &\equiv p\left[1 + \binom{(p+1)/2}{2}\left((X-3)^2 + 6(X-3) + 8\right)\right. \\
&+\binom{(p+3)/2}{4}(X-3)\left((X-3)^3 + 10(X-3)^2 + 32(X-3) + 32\right) \\
&\left.+\binom{(p+5)/2}{6}(X-3)^2\left((X-3)^4 + 14(X-3)^3 + 72(X-3)^2 + 160(X-3) + 128\right)\right] \\
&\equiv p\left[1 + \binom{(p+1)/2}{2}8 + (X-3)\left(6\binom{(p+1)/2}{2} + 32\binom{(p+3)/2}{4}\right)\right. \\
&\qquad \left.+(X-3)^2\left(\binom{(p+1)/2}{2} + 32\binom{(p+3)/2}{4} + 128\binom{(p+5)/2}{6}\right)\right] \\
&\equiv p\left[1 + (p^2-1) + (X-3)\left(\frac{p^2(p^2-1)}{12}\right) + (X-3)^2\left(\frac{p^2(p^2-1)(p^2-4)}{360}\right)\right] \\
&\equiv p^3 \pmod{p^4}.
\end{aligned}$$

In the case of $p = 5$ we get

$$K_p(X) \equiv 5\left[1 + \binom{3}{2}(X^2-1) + \binom{4}{4}(X-3)(X+1)^2(X-1)\right] \pmod{p^4}.$$

So

$$\begin{aligned} K_p(X) &\equiv 5\left[1+3\left((X-3)^2+6(X-3)+8\right)\right. \\ &\qquad \left.+(X-3)\left((X-3)^3+10(X-3)^2+32(X-3)+32\right)\right] \\ &\equiv 5\left[25+50(X-3)+35(X-3)^2\right] \\ &\equiv 125 \pmod{p^4}. \end{aligned}$$

□

4.4 The Law of Repetition for $\{C_n\}$

Note that

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

If $m > 0$, we can easily derive from the multiplicative properties of Lucas sequences mentioned in Chapter 2 that

$$2^{m-1}U_m(P,Q) \equiv mP^{m-1} \pmod{\Delta} \quad \text{and} \quad 2^{m-1}V_m(P,Q) \equiv P^m \pmod{\Delta}.$$

Thus,

$$\begin{aligned} &2^{m-1}U_m(\tilde{P}_n,\tilde{Q}_n) \equiv m\tilde{P}_n^{m-1} \pmod{\Delta C_n^2} \quad \text{and} \\ &2^{m-1}V_m(\tilde{P}_n,\tilde{Q}_n) \equiv \tilde{P}_n^m \pmod{\Delta C_n^2}. \end{aligned}$$

We may use the identity

$$2\tilde{Q}_n^{\lambda_2}U_{\lambda_1-\lambda_2}(\tilde{P}_n,\tilde{Q}_n) = U_{\lambda_1}(\tilde{P}_n,\tilde{Q}_n)V_{\lambda_2}(\tilde{P}_n,\tilde{Q}_n) - V_{\lambda_1}(\tilde{P}_n,\tilde{Q}_n)U_{\lambda_2}(\tilde{P}_n,\tilde{Q}_n)$$

as follows:

$$\begin{aligned} 2^{\lambda_1+\lambda_2-1}\tilde{Q}_n^{\lambda_2}U_{\lambda_1-\lambda_2}(\tilde{P}_n,\tilde{Q}_n) &= 2^{\lambda_1-1}U_{\lambda_1}(\tilde{P}_n,\tilde{Q}_n)2^{\lambda_2-1}V_{\lambda_2}(\tilde{P}_n,\tilde{Q}_n) \\ &\quad -2^{\lambda_1-1}V_{\lambda_1}(\tilde{P}_n,\tilde{Q}_n)2^{\lambda_2-1}U_{\lambda_2}(\tilde{P}_n,\tilde{Q}_n) \\ &\equiv \lambda_1\tilde{P}_n^{\lambda_1-1}\tilde{P}_n^{\lambda_2} - \tilde{P}_n^{\lambda_1}\lambda_2\tilde{P}_n^{\lambda_2-1} \pmod{\Delta C_n^2} \\ &\equiv (\lambda_1-\lambda_2)\tilde{P}_n^{\lambda_1+\lambda_2-1} \pmod{\Delta C_n^2}. \end{aligned}$$

Similarly, we have

$$2^{\lambda_1+\lambda_2-1}\tilde{Q}_n^{\lambda_2}V_{\lambda_1-\lambda_2}(\tilde{P}_n,\tilde{Q}_n) \equiv \tilde{P}_n^{\lambda_1+\lambda_2} \pmod{\Delta C_n^2}.$$

If $2 \nmid \Delta C_n$, then

$$\begin{aligned} \tilde{Q}_n^{\lambda_2}U_{\lambda_1-\lambda_2}(\tilde{P}_n,\tilde{Q}_n) &\equiv (\lambda_1-\lambda_2)(\tilde{P}_n/2)^{\lambda_1+\lambda_2-1} \pmod{\Delta C_n^2}, \\ \tilde{Q}_n^{\lambda_2}V_{\lambda_1-\lambda_2}(\tilde{P}_n,\tilde{Q}_n) &\equiv 2(\tilde{P}_n/2)^{\lambda_1+\lambda_2} \pmod{\Delta C_n^2}. \end{aligned}$$

When $2 \mid \Delta C_n$, we have $2 \mid \tilde{P}_n$ and $\tilde{Q}_n \equiv (\tilde{P}_n/2)^2 \pmod{\Delta C_n^2/4}$. In this case we can show by induction that

$$\begin{aligned} U_m(\tilde{P}_n,\tilde{Q}_n) &\equiv m(\tilde{P}_n/2)^{m-1} \pmod{\Delta C_n^2/4}, \\ V_m(\tilde{P}_n,\tilde{Q}_n) &\equiv 2(\tilde{P}_n/2)^m \pmod{\Delta C_n^2/4} \end{aligned}$$

and therefore

$$\tilde{Q}_n^{\lambda_2}U_{\lambda_1-\lambda_2}(\tilde{P}_n,\tilde{Q}_n) \equiv (\lambda_1-\lambda_2)(\tilde{P}_n/2)^{\lambda_1+\lambda_2-1} \pmod{\Delta C_n^2/4}, \tag{4.9}$$

$$\tilde{Q}_n^{\lambda_2}V_{\lambda_1-\lambda_2}(\tilde{P}_n,\tilde{Q}_n) \equiv 2(\tilde{P}_n/2)^{\lambda_1+\lambda_2} \pmod{\Delta C_n^2/4}. \tag{4.10}$$

It follows by (3.17) that

$$\begin{aligned} \frac{C_{mn}}{C_n} &\equiv \sum_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \left(\frac{(-1)^{\lambda_0}m(m-\lambda_0-1)!R^{n(m-\lambda_1-\lambda_2)}}{\lambda_1!\lambda_2!\lambda_3!}\right) \\ &\qquad \left(\frac{(\lambda_1-\lambda_2)\tilde{P}_n^{\lambda_1+\lambda_2-1}}{2^{\lambda_1+\lambda_2-1}}\right) \pmod{F_n}, \end{aligned}$$

where

$$F_n = \begin{cases} \Delta C_n^2 & \text{if } 2 \nmid C_n \\ \Delta C_n^2/4 & \text{if } 2 \mid C_n. \end{cases} \tag{4.11}$$

This symbol F_n and the symbol G_n introduced near the beginning of Chapter 5 should not be confused with the F_n and G_n defined in Section 3.6. So we can use the above and equation (4.4) to see

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

Thus, by our earlier results, if m is odd,

$$\frac{C_{mn}}{C_n} \equiv mR^{n(m-1)} + m \sum_{j=1}^{(m-1)/2} \binom{(m-1)/2+j}{(m-1)/2-j} 2^{-2j} R^{n(m-2j-1)}(W_n - 2R^n) (W_n + 2R^n)^j (W_n - 6R^n)^{j-1} \pmod{F_n}$$

and if m is even,

$$\frac{C_{mn}}{C_n} \equiv m \sum_{j=1}^{m/2} \frac{m}{m/2-j} \binom{m/2+j-1}{m/2-j-1} 2^{-2j+1} R^{n(m-2j)} (W_n + 2R^n)^j (W_n - 6R^n)^{j-1} \pmod{F_n}.$$

If $p \neq 2$, $p \mid C_n$ and $p \mid R$, then since $p \mid \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!}$ and $\lambda_0 + \lambda_3 \neq 0$ whenever $\lambda_1 \neq p$, we get by equation (3.17) that

$$\frac{C_{pn}}{C_n} \equiv U_p(\tilde{P}_n, \tilde{Q}_n) \pmod{p^2}.$$

Then we may use (2.14) with $m = p$ and $n = 1$ to see

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

Thus if $p^\lambda \mid\mid C_n$, then $p^{\lambda+\mu} \mid\mid C_{p^\mu n}$.

Now suppose that $p \nmid 6R$ and $p \mid C_n$. It is easy to show by use of (3.16) that

$$W_{pn} \equiv V_p(\tilde{P}_n, \tilde{Q}_n) \equiv \tilde{P}_n \equiv W_n \pmod{p}.$$

Clearly, then, $W_{pn} - 6R^{pn} \equiv W_n - 6R^n \pmod{p}$. If $p \nmid W_n - 6R^n$, then $p^2 \mid F_n$ and by Theorem 4.20

$$\frac{C_{pn}}{C_n} \equiv R^{n(p-1)} K_p(W_n/2R^n) \equiv R^{n(p-1)} p \equiv p \pmod{p^2}.$$

In this case if $p^\lambda \mid\mid C_n$, then $p^{\lambda+\mu} \mid\mid C_{p^\mu n}$.

On the other hand, if $p \mid W_n - 6R^n$ and $p \nmid \Delta$, then by Theorem 4.18 we have $p^3 \mid C_n \Rightarrow p^3 \mid F_n$. Also, if $p \mid W_n - 6R^n$ and $p \mid \Delta$, then $p^3 \mid F_n$. We then have by (4.9)

$$\tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) \equiv (\lambda_1 - \lambda_2)(\tilde{P}_n/2)^{\lambda_1+\lambda_2-1} \pmod{p^3}.$$

Further, since $p \mid \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!}$ when $\lambda_1 \neq p$, we can say

$$\begin{aligned}
\frac{C_{pn}}{C_n} &= U_p(\tilde{P}_n, \tilde{Q}_n) + \sum_{\lambda_1 \neq p} \frac{(-1)^{\lambda_0} p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(p-\lambda_1-\lambda_2)} \tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) \\
&\equiv U_p(\tilde{P}_n, \tilde{Q}_n) + \sum_{\lambda_1 \neq p} \frac{(-1)^{\lambda_0} p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} R^{n(p-\lambda_1-\lambda_2)} (\lambda_1 - \lambda_2)(\tilde{P}_n/2)^{\lambda_1+\lambda_2-1} \\
&\equiv U_p(\tilde{P}_n, \tilde{Q}_n) + R^{n(p-1)} \left[K_p(W_n/2R^n) - p(\tilde{P}_n/2R^n)^{p-1} \right] \pmod{p^4}.
\end{aligned}$$

Now,

$$2^{p-1} U_p(\tilde{P}_n, \tilde{Q}_n) \equiv p\tilde{P}_n^{p-1} + \tilde{\Delta}_n \binom{p}{3} \tilde{P}_n^{p-3} \pmod{p^4}.$$

Since $p^3 \mid C_n$ we have $p^4 \mid \tilde{\Delta}_n$, yielding

$$U_p(\tilde{P}_n, \tilde{Q}_n) \equiv p(\tilde{P}_n/2)^{p-1} \pmod{p^4},$$

and so

$$\begin{aligned}\frac{C_{pn}}{C_n} &\equiv p(\tilde{P}_n/2)^{p-1} + R^{n(p-1)}K_p(W_n/2R^n) - p(\tilde{P}_n/2)^{p-1} \pmod{p^4} \\ &\equiv R^{n(p-1)}K_p(W_n/2R^n) \pmod{p^4} \\ &\equiv (R^n)^{p-1}p^3 \equiv p^3 \pmod{p^4}.\end{aligned}$$

Thus, in this case, if $p^\lambda \mid\mid C_n$, then $p^{\lambda+3\mu} \mid\mid C_{p^\mu n}$.

We can now state the law of repetition for $\{C_n\}$. Let $p^\lambda \mid\mid C_n$ $(\lambda \geq 1)$.

- If $p = 2, 3$ then $p^{\lambda+\mu} \mid C_{p^\mu n}$.
- If $p \neq 2$ and $p \mid R$, then $p^{\lambda+\mu} \mid\mid C_{p^\mu n}$.
- If $p \nmid R$ and $p \nmid W_n - 6R^n$, then $p^{\lambda+\mu} \mid\mid C_{p^\mu n}$.
- If $p \nmid R$ and $p \mid W_n - 6R^n$, then $p^{\lambda+3\mu} \mid\mid C_{p^\mu n}$.

We next provide a closer examination of the case of $p = 3$: If $3 \mid C_n$, $3 \nmid R$ and $3 \nmid W_n - 6R^n$, then $3 \nmid W_n$. By Corollary 3.10.1 we have

$$\begin{aligned}4W_{3n} &= 3\Delta C_n^2(W_n + 2R^n) + W_n^2(W_n - 6R^n) + 24R^{3n}, \\ 4C_{3n} &= C_n(\Delta C_n^2 + 3W_n^2).\end{aligned}$$

We then can see

$$4\frac{C_{3n}}{C_n} \equiv \Delta C_n^2 + 3W_n^2 \pmod 9 \Rightarrow 4\frac{C_{3n}}{C_n} \equiv 3W_n^2 \pmod 9.$$

Hence $3 \mid\mid \frac{C_{3n}}{C_n}$ and $3 \nmid W_{3n}$. Thus, if $3^\lambda \mid\mid C_n$, then $3^{\lambda+\mu} \mid\mid C_{3^\mu n}$.

If $3 \mid C_n$, $3 \nmid R$, $3 \mid W_n - 6R^n$, then $3 \mid W_n \Rightarrow 3 \mid A_nB_n - 3R^n \Rightarrow 3 \mid A_nB_n$. Since

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

we see that if $3 \mid A_n$, then $3 \mid B_n$ and if $3 \mid B_n$, then $3 \mid A_n$. So we have $9 \mid A_nB_n$ and this implies $3 \mid\mid W_n$. Further $27 \mid\mid 3W_n^2$ and $3 \mid W_{3n}$. Thus, if $3^\lambda \mid\mid C_n$ and $\lambda \geq 2$, then

$$4\frac{C_{3n}}{C_n} \equiv 3W_n^2 \pmod{81}.$$

It follows that $3^3 \mid\mid C_{3n}/C_n \Rightarrow 3^{\lambda+3\mu} \mid\mid C_{3^\mu n}$. If $3^\lambda = 3$, then $3^{\lambda+3\mu} \mid C_{3^\mu n}$.

We next provide a similar examination of the $p = 2$ case.

Case 1. $2 \mid R$.

If $4 \mid C_n$, then since $(W_n^2 - \Delta C_n^2)/4 \in \mathbb{Z}$ we have $2 \mid W_n$; furthermore, $2 \mid A_nB_n$ as $A_nB_n = W_n + 3R^n$. Also

$$\begin{aligned} 27\Delta C_n^2 &= 4(A_n^2 - 3B_n^2)^3 - (27R^n + 2A_n^3 - 9A_nB_n)^2 \\ &= 4(A_n^2 - 3B_n^2)^3 - (2A_n^3 - 9W_n)^2. \end{aligned}$$

We have in this case that $A_n^2 - 3B_n^2$ is odd since $2 \nmid Q \Rightarrow 2 \nmid B_n$ and therefore $2 \mid A_n$. We can use this to see that

$$27\Delta C_n^2 \equiv 4 - W_n^2 \pmod{8}.$$

Thus $2 \mid\mid W_n \Rightarrow 2 \mid\mid W_n + 2R^n$. But this means $2 \mid\mid C_{2n}/C_n$ since $C_{2n} = C_n(W_n + 2R^n)$. We may conclude $2^{\mu+\lambda} \mid\mid C_{2^\mu n}$, if $2^\lambda \mid\mid C_n$ and $\lambda \geq 2$. If $2 \mid R$ and $\lambda = 1$, we can only show that $2^{\mu+\lambda} \mid C_{2^\mu n}$.

Case 2. $2 \nmid R$.

If $4 \mid C_n$, then $2 \mid W_n \Rightarrow 2 \mid A_nB_n - 3R^n \Rightarrow 2 \nmid A_nB_n \Rightarrow 2 \mid A_n^2 - 3B_n$. So

$$27\Delta C_n^2 \equiv -(2A_n^3 - 9W_n)^2 \pmod{8}.$$

Now

$$\begin{aligned} 2A_n^3 - 9W_n &\equiv 2 - W_n \pmod 4 \\ &\Rightarrow (2A_n^3 - 9W_n)^2 \equiv (2 - W_n)^2 \pmod 8 \\ &\Rightarrow 27\Delta C_n^2 \equiv -(2 - W_n)^2 \pmod 8. \end{aligned}$$

If $4 \mid C_n$, then $8 \mid (2 - W_n)^2 \Rightarrow 4 \mid 2 - W_n \Rightarrow 2 \mid\mid W_n$. Hence $4 \mid W_n + 2R^n \Rightarrow 4 \mid C_{2n}/C_n \Rightarrow 2^{\lambda+2\mu} \mid C_{2^\mu n}$ if $2^\lambda \mid\mid C_n$ and $\lambda \geq 2$. If $2 \mid\mid C_n$, then $2 \mid C_{2n}/C_n$ and $4 \mid C_{2n}$. Hence $2^{2\mu} \mid C_{2^\mu n}$ when $\mu \geq 1$.

Since $(W_n, C_n, R) \mid 2$, we can now revise the *law of repetition for* $\{C_n\}$ in the theorem below.

Theorem 4.21. *Let* $p^\lambda \mid\mid C_n$ *and* $(\lambda \geq 1)$

- *If* $p = 2$ *we have two cases:*
  - *If* $2 \mid R$, *then*

$$2^{\lambda+\mu} \mid\mid C_{2^\mu n} \quad \textit{for } \lambda > 1,$$
$$2^{\lambda+\mu} \mid C_{2^\mu n} \quad \textit{for } \lambda = 1.$$

  - *If* $2 \nmid R$, *then*

$$2^{\lambda+2\mu} \mid C_{2^\mu n} \quad \textit{for } \lambda > 1,$$
$$2^{2\mu} \mid C_{2^\mu n} \quad \textit{for } \lambda = 1.$$

- *If* $p \neq 2$, *then*

$$p^{\lambda+\mu} \mid\mid C_{p^\mu n} \quad \textit{when } p \nmid W_n - 6R^n.$$

- *If $p \neq 2$ and $p^\lambda \neq 3$, then*

$$p^{\lambda+3\mu} \mid\mid C_{p^\mu n} \quad \textit{when } p \mid W_n - 6R^n.$$

- *If $p^\lambda = 3$, then*

$$3^{\lambda+3\mu} \mid C_{3^\mu n} \quad \textit{when } p \mid W_n.$$

If $p = 2$ and $2 \nmid \Delta R$, we have some additional special cases. When $\lambda \geq 4$, we can only have $8 \mid\mid W_n - 6R^n$ or $16 \mid W_n - 6R^n$ by Theorem 4.19. If $16 \mid W_n - 6R^n$, then since $W_n + 2R^n = W_n - 6R^n + 8R^n$, we see that $2^3 \mid\mid W_n + 2R^n \Rightarrow 2^3 \mid\mid C_{2n}/C_n$, as $C_{2n} = C_n(W_n + 2R^n)$. Also, $16 \mid W_{2n} - 6R^{2n}$. Thus $2^{\lambda+3\mu} \mid\mid C_{2^\mu n}$ by induction.

On the other hand, if $8 \mid\mid W_n - 6R^n$, then since

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

we observe that $32 \mid W_{2n} - 6R^{2n}$. Further, since $W_{2n} - 6R^{2n} + 8R^{2n} = W_{2n} + 2R^{2n}$ and $32 \mid W_{2n} - 6R^{2n}$, we have $8 \mid\mid W_{2n} + 2R^{2n}$. Now, both $(W_n - 6R^n)/8$ and R^n are odd. Thus

$$2 \mid \frac{W_n - 6R^n}{8} + R^n \Rightarrow 8 \cdot 2 \mid 8\left(\frac{W_n - 6R^n}{8} + R^n\right) \Rightarrow 16 \mid W_n + 2R^n.$$

Finally, if $2^\nu \mid\mid W_n + 2R^n$, we get $2^\nu \mid\mid C_{2n}/C_n \Rightarrow 2^{\nu+\lambda} \mid\mid C_{2n}$, then

$$2^{3(\mu-1)+\nu+\lambda} \mid\mid C_{2^\mu n}$$

by our earlier observation and induction on μ.

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 $p^\lambda \mid\mid U_n$. Unfortunately, this result does not generalize

to C_n. For example, if $p \nmid W_n - 6R^n$ and $p \nmid 2R$, it is possible for $p^\lambda \mid\mid C_n$ and $p^{\lambda+1} \mid C_{mn}$, where $p \nmid m$. We note that

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

If $V_m(W_n/2R^n - 1, 1) \equiv 2 \pmod{p}$ and $p \nmid m$, then $p \mid C_{mn}/C_n$. We also have the equality of the two Legendre symbols

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

So if

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

then

$$V_{p-1}(W_n/2R^n - 1, 1) \equiv 2 \pmod{p} \Rightarrow p \mid C_{(p-1)n}/C_n \quad \text{and} \quad p \nmid p - 1.$$

Also, if

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

then

$$V_{p+1}(W_n/2R^n - 1, 1) \equiv 2 \pmod{p} \Rightarrow p \mid C_{(p+1)n}/C_n \quad \text{and} \quad p \nmid p + 1.$$

Lastly, if

$$\left(\frac{(W_n - 6R^n)(W_n + 2R^n)}{p}\right) = 0,$$

then $p \mid (W_n/2R^n - 1)^2 - 4 \Rightarrow W_n/2R^n - 1 \equiv \pm 2 \pmod{p}$. In this case, $V_2(W_n/2R^n - 1, 1) \equiv (W_n/2R^n - 1)^2 - 2 \equiv (W_n/2R^n - 1)^2 - 4 + 2 \equiv 2 \pmod{p}$. So then $p \mid C_{2n}/C_n$ and $2 \nmid p$.

4.5 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 $p \nmid R$ in what follows.

We recall 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.

Case one occurs when $p \mid P^2-3Q$. 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 $\mathbb{F}_p$,

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

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 $p \mid C_n \Leftrightarrow p \mid n$. Also, if $p \mid C_n$, then $p \mid W_n - 6R^n$.

Case two occurs when $p \nmid P^2-3Q$. In this case $f(x) \equiv (x-a)^2(x-b) \pmod{p}$, where

$$a \equiv \frac{PQ-9R}{2(P^2-3Q)} \pmod{p} \quad \text{and} \quad b \equiv \frac{P^3-4PQ+9R}{P^2-3Q} \pmod{p}. \tag{4.12}$$

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, $2a + b \equiv P \pmod{p} \Rightarrow a + b \equiv P - a \pmod{p}$. 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 $(\frac{\Delta'}{p}) = 1$, 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 $p \mid C_n \Leftrightarrow p \mid n$ or $p \mid U_n(P', Q')$ since $p \nmid a$. If $p \mid a$ or $p \mid Q'$, then $p \mid R$, 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 $p \mid C_n \Leftrightarrow$ 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.

We have already shown that $r(2)$ always exists and is unique. The case for $p = 3$ can be handled explicitly by calculation. The results are given in Table 4.1, where we assume $3 \nmid R$ and P, Q, R are given modulo 3.

Table 4.1: Ranks of apparition for $p = 3$

P	Q	R	$\Delta \pmod 3$	$C_m \equiv 0 \pmod 3$ iff	Corresponding W_m
2	2	2	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
2	2	1	0	$m \equiv 0 \pmod 2$ or $m \equiv 0 \pmod 3$	$W_2 \equiv 0 \pmod 3$ and $W_3 \equiv 1 \pmod 3$
2	1	2	2	$m \equiv 0 \pmod 2$	$W_2 \equiv 1 \pmod 3$
2	1	1	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
2	0	2	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
2	0	1	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
1	2	2	0	$m \equiv 0 \pmod 2$ or $m \equiv 0 \pmod 3$	$W_2 \equiv 0 \pmod 3$ and $W_3 \equiv 2 \pmod 3$
1	2	1	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
1	1	2	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
1	1	1	2	$m \equiv 0 \pmod 2$	$W_2 \equiv 1 \pmod 3$
1	0	2	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
1	0	1	2	$m \equiv 0 \pmod 4$	$W_4 \equiv 1 \pmod 3$
0	2	2	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
0	2	1	1	$m \equiv 0 \pmod{13}$	$W_{13} \equiv 0 \pmod 3$
0	1	2	2	$m \equiv 0 \pmod 4$	$W_4 \equiv 1 \pmod 3$
0	1	1	2	$m \equiv 0 \pmod 4$	$W_4 \equiv 1 \pmod 3$
0	0	2	0	$m \equiv 0 \pmod 3$	$W_3 \equiv 0 \pmod 3$
0	0	1	0	$m \equiv 0 \pmod 3$	$W_3 \equiv 0 \pmod 3$

From this we see that there must always exist 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 $r(3) \mid n$.

4.6 Solutions of the Cubic

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*.

Suppose G is the galois group of the polynomial $f(x)$. There are four possibilities for G: $G_1 = \{1\}$, G_2 a group of order 2, G_3 a group of order 3 or G_6 the dihedral group of order 6. In G_1 there is only one conjugacy class, in G_2 there are two conjugacy classes, in G_3 there are two conjugacy classes and in G_6 there are three conjugacy classes. Let $\pi(x)$ denote the number of primes up to x and for a fixed $f(x)$ denote by $\pi_S(x)$, $\pi_Q(x)$, $\pi_I(x)$ the number of S, Q, I primes up to x, respectively. By the Chebotarëv density theorem [SHWL96] we know that if $G \simeq G_1$, then all the primes are S primes. If $G \simeq G_2$, then

$$\lim_{x\to\infty} \frac{\pi_S(x)}{\pi(x)} = \frac{1}{2}, \quad \text{and} \quad \lim_{x\to\infty} \frac{\pi_Q(x)}{\pi(x)} = \frac{1}{2}.$$

If $G \simeq G_3$, then

$$\lim_{x\to\infty} \frac{\pi_S(x)}{\pi(x)} = \frac{1}{3}, \quad \text{and} \quad \lim_{x\to\infty} \frac{\pi_I(x)}{\pi(x)} = \frac{2}{3}.$$

Finally, if $G \simeq G_6$, then

$$\lim_{x\to\infty} \frac{\pi_S(x)}{\pi(x)} = \frac{1}{6}, \quad \lim_{x\to\infty} \frac{\pi_Q(x)}{\pi(x)} = \frac{1}{2} \quad \text{and} \quad \lim_{x\to\infty} \frac{\pi_I(x)}{\pi(x)} = \frac{1}{3}.$$

Determining which of these types of prime p is important, since its type dictates where $C_n = 0$ 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]). As the results concerning this problem are widely scattered, we will present a self-contained version here. Remember that $\delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$, $\Delta = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$, and $-27\Delta = (2P^3 - 9QR + 27R)^2 - 4(P^2-3Q)^3$.

If p is a Q prime, we may assume that $\alpha \in \mathbb{F}_p$, β, $\gamma \in \mathbb{F}_{p^2}\backslash\mathbb{F}_p$. Hence $\alpha^p = \alpha$, $\beta^p = \gamma$ and $\gamma^p = \beta$. Then, in $\mathbb{K}$,

$$\begin{aligned} \delta^p &= (\alpha-\beta)^p(\beta-\gamma)^p(\gamma-\alpha)^p \\ &= (\alpha^p-\beta^p)(\beta^p-\gamma^p)(\gamma^p-\alpha^p) \\ &= (\alpha-\gamma)(\gamma-\beta)(\beta-\alpha) = -\delta. \end{aligned}$$

So $\delta^{p-1} = -1 \Leftrightarrow \Delta^{(p-1)/2} = -1 \Leftrightarrow (\frac{\Delta}{p}) = -1$.

In the other cases, we get either $\alpha^p = \alpha$, $\beta^p = \beta$, $\gamma^p = \gamma$ or $\alpha^p = \beta$, $\beta^p = \gamma$, $\gamma^p = \alpha$. In either case $\delta^p = \delta \Rightarrow (\frac{\Delta}{p}) = 1$. Thus p is a Q prime if and only if $(\frac{\Delta}{p}) = -1$.

Now assume $(\frac{\Delta}{p}) = 1$, and let $A = 2P^3 - 9QR + 27R$ and $B = P^2 - 3Q$. Then $-27\Delta = A^2 - 4B^3$. Let $\mathbb{K}$ be the splitting field of $f(x) \in \mathbb{F}_p[x]$. Then $\mathbb{K} = \mathbb{F}_p$ or $\mathbb{F}_{p^3}$. In either case $\mathbb{K}$ is a subfield of $\mathbb{L} = \mathbb{F}_{p^6}$. Now let $\mathbb{F}_{p^6}^* = \langle\lambda\rangle$ for some primitive element λ of $\mathbb{F}_{p^6}^*$. Put $\zeta = \lambda^{(p^6-1)/3}$, then $\zeta \neq 1$ and $\zeta^3 = 1 \Rightarrow (\zeta-1)(\zeta^2+\zeta+1) = 0 \Rightarrow \zeta^2+\zeta+1 = 0$. This implies that $\alpha\beta(\zeta^2+\zeta+1) = 0 \Rightarrow \zeta^2\alpha\beta + \zeta\alpha\beta = -\alpha\beta$. Put

$$\begin{aligned} L_1 &= \alpha + \zeta\beta + \zeta^2\gamma \in \mathbb{L} \\ L_2 &= \alpha + \zeta^2\beta + \zeta\gamma \in \mathbb{L}. \end{aligned}$$

Then, $L_1L_2 = B \in \mathbb{F}_p$ and $L_1^3 + L_2^3 = A \in \mathbb{F}_p$. Thus L_1^3, L_2^3 are the zeros of $x^2 - Ax + B^3 \in \mathbb{F}_p[x]$.

Now since, $(\frac{\Delta}{p}) = 1$ and $\delta^2 = \Delta$ we have $\delta \in \mathbb{F}_p$. If we put $\rho = 3(\zeta - \zeta^2)\delta$, then $\rho^2 = -27\Delta$ and $\rho \in \mathbb{F}_{p^2}$. So $\rho^2 = -27\Delta = A^2 - 4B^3 = (L_1^3 + L_2^3)^2 - 4L_1^3L_2^3$. Notice $(L_1^3 - L_2^3)^2 = (L_1^3)^2 - 2L_1^3L_2^3 + (L_2^3)^2 = (L_1^3)^2 + 2L_1^3L_2^3 + (L_2^3)^2 - 4L_1^3L_2^3 = A^2 - 4B^3 = -27\Delta \Rightarrow L_1^3 - L_2^3 = \pm\rho$. This implies

$$\begin{aligned} 2L_1^3 &= A \pm \rho \\ 2L_2^3 &= A \mp \rho. \end{aligned}$$

Now since L_1^3, L_2^3 are the zeros of $x^2 - Ax + B^3$ we have

$$V_n(A, B^3) = (L_1^3)^n + (L_2^3)^n \quad \text{and} \quad U_n(A, B^3) = \frac{(L_1^3)^n - (L_2^3)^n}{L_1^3 - L_2^3}.$$

From this we see that

$$2(L_1^3)^n = V_n(A, B^3) \pm \rho U_n(A, B^3) \tag{4.13}$$

and

$$2(L_2^3)^n = V_n(A, B^3) \mp \rho U_n(A, B^3). \tag{4.14}$$

Suppose $p \equiv 1 \pmod 3$. If $\mathbb{K} = \mathbb{F}_p$ (p is an S prime) then

$$L_1^p = \alpha^p + \zeta^p\beta^p + \zeta^{2p}\gamma^p = \alpha + \zeta^{3n}\zeta\beta + \zeta^{6n}\zeta^2\gamma = L_1.$$

Similarly $L_2^p = L_2$. This gives us $L_1^{3(\frac{p-1}{3})} = 1$ and $L_2^{3(\frac{p-1}{3})} = 1$.

If $B \neq 0$, then $L_1 \neq 0$ and $L_2 \neq 0$. If $B = 0$, then $L_1 = 0$ or $L_2 = 0$, but not both since $-27\Delta = (L_1^3 - L_2^3)^2$. Without loss of generality assume $L_1 = 0$, then $L_2^3 = A$.

In this case p is an S prime if and only if $A^{\frac{p-1}{3}} \equiv 1 \pmod{p}$. Thus, if $(\frac{\Delta}{p}) = 1$, $p \mid B$, then p is an S prime if and only if $A^{\frac{p-1}{3}} \equiv 1 \pmod{p}$.

If $p \nmid B$, then $L_1^{3(\frac{p-1}{3})} = L_2^{3(\frac{p-1}{3})}$. Use the above and equations (4.13) and (4.14) to see that $U_{\frac{p-1}{3}}(A, B^3) = 0$.

Now suppose $U_{\frac{p-1}{3}}(A, B^3) \equiv 0 \pmod{p} \Rightarrow L_1^{3(\frac{p-1}{3})} = L_2^{3(\frac{p-1}{3})}$ in $\mathbb{L}$ by (4.13) and (4.14). Since $p \nmid B$, we have $(L_1/L_2)^{p-1} = 1 \Rightarrow (L_1/L_2)^p = (L_1/L_2)$, and therefore $L_1/L_2 \in \mathbb{F}_p$. Since $L_1 L_2 \in \mathbb{F}_p$ we get $L_1^2,\ L_2^2 \in \mathbb{F}_p$. Also $(L_1^3 - L_2^3)^2 \equiv -27\Delta \pmod{p}$ and $(\frac{-27\Delta}{p}) = (\frac{-3}{p})(\frac{3^2}{p})(\frac{\Delta}{p}) = 1$ gives us $L_1^3 - L_2^3 \in \mathbb{F}_p$ and $L_1^3 - L_2^3 \neq 0$. So $L_1^3 - L_2^3 = (L_1 - L_2)(L_1^2 + L_2^2 + L_1 L_2)$ and $L_1^2 + L_2^2 + L_1 L_1 \in \mathbb{F}_p \Rightarrow L_1 - L_2 \in \mathbb{F}_p$. But $L_1^2 - L_2^2 \in \mathbb{F}_p \Rightarrow L_1 + L_2 \in \mathbb{F}_p \Rightarrow L_1,\ L_2 \in \mathbb{F}_p$. Since $\zeta^p = \zeta$, we have $\zeta \in \mathbb{F}_p$, and it then follows that $\alpha,\ \beta,\ \gamma \in \mathbb{F}_p \Rightarrow p$ is a S prime.

Suppose $p \equiv -1 \pmod{3}$ and $\mathbb{K} = \mathbb{F}_p$. Then $B \neq 0$. For if $B = 0$ we get $-27\Delta = A^2 - 4B^3 = A^2$ and $(\frac{-27\Delta}{p}) = 1$. This is a contradiction since $p \equiv -1 \pmod{3} \Rightarrow (\frac{-27\Delta}{p}) = -1$. Now,

$$L_1^p = (\alpha + \zeta\beta + \zeta^2\gamma)^p = \alpha^p + \zeta^p\beta^p + \zeta^{2p}\gamma^p.$$

Thus if p is an S prime, then $L_1^p = L_2$ and $L_2^p = L_1 \Rightarrow L_1^{p^2} = L_1$ and $L_2^{p^2} = L_2 \Rightarrow (L_1^{3(p-1)})^{(p+1)/3} = 1$, $(L_2^{3(p-1)})^{(p+1)/3} = 1 \Rightarrow (L_2^3/L_1^3)^{(p+1)/3} = 1 \Rightarrow (L_2^3)^{(p+1)/3} = (L_1^3)^{(p+1)/3} \Rightarrow U_{\frac{p+1}{3}}(A, B^3) = 0$.

Now if $U_{\frac{p+1}{3}}(A, B^3) \equiv 0 \pmod{p}$, then $L_2^{3\frac{p+1}{3}} = L_1^{3\frac{p+1}{3}}$ in $\mathbb{L} \Rightarrow (L_2/L_1)^{p+1} = 1 \Rightarrow L_2^{p+1} = L_1^{p+1} \Rightarrow (L_2/L_1)^p = (L_1/L_2)$. So $(L_2/L_1)^{p^2} = (L_2/L_1)$. Hence $L_2/L_1 \in \mathbb{F}_{p^2}$ and $L_1/L_2 \in \mathbb{F}_{p^2}$. Since $\zeta^{p^2} = \zeta$, we can employ our previous reasoning to establish that $\alpha^{p^2} = \alpha$, $\beta^{p^2} = \beta$, $\gamma^{p^2} = \gamma$. Since $(\frac{\Delta}{p}) = 1$, we must have that α, β, γ are in $\mathbb{F}_p$ or $\mathbb{F}_{p^3}$. If p is an I prime, then $\alpha^p = \beta$, $\beta^p = \gamma$, $\gamma^p = \alpha \Rightarrow \alpha^{p^2} = \gamma$, $\beta^{p^2} = \alpha$,

$\gamma^{p^2} = \beta$. But then $\alpha^{p^2} = \gamma = \alpha$, and $p \mid \Delta$, which is a contradiction. Hence p is not an I prime $\Rightarrow$ p is an S prime.

It follows that if $p \equiv \epsilon \pmod 3$ ($\epsilon \in \{-1, 1\}$), then if $(\frac{\Delta}{p}) = 1$ and $p \nmid B$, we have that p is an S prime if and only if $U_{\frac{p-\epsilon}{3}}(A, B^3) \equiv 0 \pmod p$.

Thus, we have proved the following theorem.

Theorem 4.22. *Suppose p is a prime and $p \nmid 6\Delta R$. If $(\frac{\Delta}{p}) = -1$, then p is a Q prime. If $(\frac{\Delta}{p}) = 1$, $p \equiv \epsilon \pmod 3$, $A = 2P^3 - 9QR + 27R$, $B = P^3 - 3Q$ 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 $\{C_n\}$. We first prove the following simple lemma.

Lemma 4.23. *Let p be a prime such that $p \nmid 2R\Delta$, $\mathbb{K}$ be the splitting field for $f(x) \in \mathbb{F}_p[x]$ and α, β, γ be the zeros of $f(x)$ in $\mathbb{K}$. If $\alpha^n = \beta^n$ and $\alpha^m = \beta^m$, then $\alpha^s = \beta^s$, where $n \equiv s \pmod m$.*

Proof. We have $n = qm + s$ and $\alpha^{qm+s} = \beta^{qm+s}$. Since $\alpha^{qm} = \beta^{qm}$ and $R \neq 0$, we get $\alpha^s = \beta^s$.

□

We next determine the number of ranks of apparition of a Q prime.

Theorem 4.24. *Let p be a Q prime and α, β, γ 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 $\beta^m = \beta^{pm}$.*

Proof. Since p is a Q prime, $f(x)$ has the 3 zeros, namely, α in $\mathbb{F}_p$ and β, γ in $\mathbb{F}_{p^2}$ such that $\alpha^p = \alpha$, $\beta^p = \gamma$, $\gamma^p = \beta$.

Assume $p \mid C_m$. It follows that $\alpha^m = \beta^m$, $\beta^m = \gamma^m$ or $\gamma^m = \alpha^m$. If $\alpha^m = \beta^m$, then $\beta^m \in \mathbb{F}_p \Rightarrow \beta^{pm} = \beta^m$. If $\beta^m = \gamma^m$, then $\beta^{pm} = \gamma^{pm} = \beta^m$. If $\gamma^m = \alpha^m$, then $\beta^{pm} = \gamma^m = \alpha^m \Rightarrow \beta^{pm} \in \mathbb{F}_p \Rightarrow \beta^{p^2 m} = \beta^{pm} \Rightarrow \beta^m = \beta^{pm}$.

On the other hand if $\beta^m = \beta^{pm}$, then $\beta^m = \gamma^m \Rightarrow p \mid C_m$. □

Corollary 4.24.1. *If p is a Q prime, then $p \mid C_{p+1}$.*

Proof. This follows directly from the theorem by noting,

$$\beta^{p+1} = \beta\beta^p = \beta^{p^2}\beta^p = \beta^{p^2+p} = \beta^{p(p+1)}.$$

□

Corollary 4.24.2. *Let p be a Q prime, then p can only have one rank, r, of apparition in $\{C_n\}$ and $r \mid p+1$.*

Proof. Suppose r is the minimal rank of apparition of p and $p \mid C_m$. We must have $\beta^m = \beta^{pm}$ by Theorem 4.24. Put $m = qr + s$ such that $0 < s < r$. We have $\beta^{qr+s} = \beta^{pqr+ps}$. Now $\beta^r = \beta^{rp} \Rightarrow \beta^{qr} = \beta^{qrp} \neq 0$. So $\beta^s = \beta^{ps} \Rightarrow p \mid C_s$ contradicting the definition of r. It follows that $s = 0$ and $r \mid m$. Thus, there can only be one rank of apparition r for p and $r \mid p+1$.

□

Corollary 4.24.3. *If p is a Q prime and r is its rank of apparition in $\{C_n\}$, then if $p \mid C_n$, we must have $r \mid n$.*

Proof. The proof follows at once from Corollary 4.24.2; if there existed an n with $r \nmid n$ then there would be another rank of apparition. □

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

$$W_{p^2-1} \equiv 6 \pmod{p}. \tag{4.15}$$

Theorem 4.25. *If p is an I prime, then $p \mid C_{p^2+p+1}$.*

Proof. Since p is an I prime,

$$\alpha^p = \beta, \quad \beta^p = \gamma \quad \text{and} \quad \gamma^p = \alpha.$$

So

$$\alpha^{p^2+p+1} = \beta^{p^2+p+1} = \gamma^{p^2+p+1} = R.$$

Hence the result follows. □

Under the same conditions we can see

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

Corollary 4.25.1. *Let p be an I prime, then p can only have one rank, r, of apparition in $\{C_n\}$ and $r \mid p^2+p+1$.*

Proof. Suppose r is the minimal rank of apparition of p for $\{C_n\}$. So, without loss of generality $\alpha^r = \beta^r \Rightarrow \alpha^{pr} = \beta^{pr} \Rightarrow \beta^r = \gamma^r \Rightarrow \alpha^r = \beta^r = \gamma^r$. If $p \mid C_m$, then $\alpha^m = \beta^m$, $\beta^m = \gamma^m$ or $\gamma^m = \alpha^m$. Thus, if $m = qr + s$ and $0 \leq s < r$, then $p \mid C_s$ by Lemma 4.23. By the definition of r, we must have $s = 0$ and $r \mid m$. Thus, there can only be one rank of apparition of p in $\{C_n\}$. Furthermore, since $p \mid C_{p^2+p+1}$, we get $r \mid p^2+p+1$.

□

Corollary 4.25.2. *If p is an I prime and r is its rank of apparition in $\{C_n\}$, then if $p \mid C_n$, we must have $r \mid n$.*

Thus, the situation with Q and I primes parallels that concerning 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 from this as we see below.

Theorem 4.26. *Let $p \nmid 6\Delta R$ and p be an S prime, then $p \mid C_{p-1}$.*

Proof. Since $\alpha, \beta, \gamma \in \mathbb{F}_p \Rightarrow \alpha^{p-1} = \beta^{p-1} = \gamma^{p-1} = 1$. Hence, $p \mid C_{p-1}$. □

Once more we note that

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

under these circumstances.

Corollary 4.26.1. *Let $p \nmid 6\Delta R$ and p be an S prime, then p may have at most 3 ranks of apparition in $\{C_n\}$ and each rank of apparition divides $p-1$.*

Proof. Let r_1 be any rank of apparition of p in $\{C_n\}$. If $p \mid C_{r_1}$, then $\alpha^{r_1} = \beta^{r_1}$ or $\beta^{r_1} = \gamma^{r_1}$ or $\gamma^{r_1} = \alpha^{r_1}$. Without loss of generality assume $\alpha^{r_1} = \beta^{r_1}$. Since p is an S prime, we know that $\alpha^{p-1} = \beta^{p-1}$. Suppose r_1 is the least positive integer such that $\alpha^{r_1} = \beta^{r_1}$. Let $p-1 = qr_1+s$ such that $0 < s < r_1$. Then $\alpha^{qr_1+s} = \beta^{qr_1+s} \Rightarrow \alpha^s = \beta^s$. This is a contradiction, thus $r_1 \mid p-1$.

Now suppose r_1 is the minimal rank of apparition. Further, suppose $p \mid C_{r_2}$ and $r_1 \nmid r_2$. We know $\alpha^{r_2} \neq \beta^{r_2}$, for if $\alpha^{r_2} = \beta^{r_2}$, then $r_2 = r_1 q + s$ where $0 < s < r_1$ and by Lemma 4.23 $\alpha^s = \beta^s$, which is a contradiction. Thus without loss of generality

$\beta^{r_2} = \gamma^{r_2}$ and let us assume r_2 is the least positive integer such that this is true. We know by the above reasoning that $r_2 \mid p-1$. Continue in this fashion, letting $r_3 \mid C_{r_3}$ and $r_1 \nmid r_3$, $r_2 \nmid r_3$. Again, by Lemma 4.23 $\gamma^{r_3} = \alpha^{r_3}$. Also, if we assume r_3 to be the least positive integer such that $\gamma^{r_3} = \alpha^{r_3}$, then $r_3 \mid p-1$. Now if we try to define r_4 such that $r_4 \mid C_{r_4}$ and $r_1 \nmid r_4$, $r_2 \nmid r_4$, $r_3 \nmid r_4$, then $\alpha^{r_4} = \beta^{r_4}$, $\beta^{r_4} = \gamma^{r_4}$ or $\gamma^{r_4} = \alpha^{r_4}$. None of which is possible by Lemma 4.23. Thus there can be at most 3 ranks of apparition in this case.

□

Corollary 4.26.2. *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.*

Proof. Without loss of generality we may suppose that $\alpha^n = \beta^n$ in $\mathbb{K}$. We have already seen that if r_1 is the least positive integer for which $\alpha^{r_1} = \beta^{r_1}$, then r_1 is a rank of apparition of p in $\{C_n\}$. Furthermore, by Lemma 4.23 we must have $\alpha^s = \beta^s$, where $n = qr_1 + s$ $(0 \leq s < r_1)$. If $s > 0$, we get a contradiction to the definition of r_1; thus, $s = 0$ and $r_1 \mid n$. □

In the next theorem, we show that the case of 3 ranks of apparition can occur infinitely often.

Theorem 4.27. *Let p be a prime such that $p = 2^\kappa k_1 k_2 + 1$, where k_1, k_2 are odd, $(k_1, k_2) = 1$, and k_1, $k_2 > 1$. There exists a set of values for P, Q, R such that $\{C_n\}$ has 3 ranks of apparition.*

Proof. We select any primitive root g of p and any integer r. In $\mathbb{F}_p$, put

$$\alpha = g^r, \quad \beta = g^{r+k_1}, \quad \gamma = g^{r+k_1+k_2}.$$

From these we can easily produce corresponding P, Q, $R \pmod p$. Note that if we put

$$r_1 = 2^\kappa k_2, \;\; r_2 = 2^\kappa k_1, \;\; r_3 = \frac{2^{\kappa-1}k_1k_2}{(2^{\kappa-1}k_1k_2, (k_1+k_2)/2)},$$

then

$$\alpha^{r_1} = \beta^{r_1}, \;\; \beta^{r_2} = \gamma^{r_2}, \;\; \gamma^{r_3} = \alpha^{r_3}.$$

Thus

$$C_{r_1}, \;\; C_{r_2}, \;\; C_{r_3} \equiv 0 \pmod p.$$

Furthermore, none of r_2, r_2, r_3 divides any of the others. Thus, there must be three ranks of apparition for $\{C_n\}$. □

We remark that there exists an infinitude of distinct primes satisfying the conditions of the theorem. For if we put $k_2 = 2xk_1 + 1$ for a fixed odd $k_1 > 1$, then by Dirichlet's theorem there must exist an infinitude of values of x for any fixed $\kappa \geq 1$ such that

$$2^\kappa k_1k_2 + 1 = 2^\kappa(2xk_1+1)k_1 + 1 = 2^{\kappa+1}k_1^2x + 2^\kappa k_1 + 1$$

is a prime.

Theorem 4.28. *Let p be an S prime and $p \equiv 1 \pmod 3$. Suppose that $R^{\frac{p-1}{3}} \not\equiv 1 \pmod p$. Then there is one and only one rank of apparition, r, of p such that $r \mid \frac{p-1}{3}$.*

Proof. Since $p \equiv 1 \pmod 3$ we can let $\zeta^2+\zeta+1 = 0$ in $\mathbb{F}_p$. Since $R^{\frac{p-1}{3}} \not\equiv 1 \pmod p$, we know that

$$\alpha^{\frac{p-1}{3}} = \zeta^i, \quad \beta^{\frac{p-1}{3}} = \zeta^j, \quad \gamma^{\frac{p-1}{3}} = \zeta^k,$$

where $3 \nmid i+j+k$. Since i, j, k cannot all be the same or all different modulo 3, we must have exactly two equal modulo 3. Without loss of generality suppose $i = j \neq k$.

Then $\alpha^{\frac{p-1}{3}} = \beta^{\frac{p-1}{3}} \Rightarrow p \mid C_{\frac{p-1}{3}} \Rightarrow \exists$ a rank of apparition r of p such that $r \mid \frac{p-1}{3}$. Thus if $\alpha^n = \beta^n$, then $r \mid n$. Suppose r_1 is another rank of apparition of p such that $r_1 \neq r$. If $\alpha^{r_1} = \beta^{r_1}$, then $r \mid r_1 \Rightarrow r = r_1$, which is a contradiction.

Thus we must have $\beta^{r_1} = \gamma^{r_1}$ or $\alpha^{r_1} = \gamma^{r_1}$. If $r_1 \mid \frac{p-1}{3}$, then $\beta^{\frac{p-1}{3}} = \gamma^{\frac{p-1}{3}}$ or $\alpha^{\frac{p-1}{3}} = \gamma^{\frac{p-1}{3}}$, neither of which is possible, as k is distinct modulo 3 from i and j.

□

Chapter 5

Arithmetic Properties of $\{D_n\}$

5.1 Preliminary Results for the Law of Repetition for $\{D_n\}$

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 also noted in Section 4.6 that 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 α, β, γ, we see that the corresponding formula involving α, β 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 α^n, β^n, γ^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,

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

Notice that by Theorem 4.5 and Lemma 4.6 we have

$$(D_n, R) \mid 2. \tag{5.1}$$

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. In order to derive the law of repetition for $\{D_n\}$ we will first develop some results for the sequence $\{L_m\}$ in the same way we derived a law of repetition for $\{C_n\}$ by first using the sequence $\{K_m\}$.

Let

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

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

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

By Waring's theorem,

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

where α_1, α_2, α_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 $2 \nmid m$, then by (4.6) we have

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

On the other hand, if $2 \mid m$, then by (4.7) we have

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

Now, by using results similar to those in Section 4.4 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

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

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

$$\begin{aligned} W_{mn} &\equiv 2R^{mn} \sum \frac{(-1)^{\lambda_0} m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} \left(\frac{W_n}{2R^n}\right)^{\lambda_1+\lambda_2} \pmod{F_n} \quad (5.2) \\ &\equiv 2R^{mn} L_m(W_n/2R^n) \pmod{F_n}. \quad (5.3) \end{aligned}$$

If m is odd,

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

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,

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

Thus, $W_{mn} \equiv 6R^{mn} \pmod{G_n} \Rightarrow G_n \mid W_{mn} - 6R^{mn}$.

It follows that if $\gamma = 0$, then $D_n \mid D_{nm}$.

If $\gamma = 1$, then since $2 \mid (W_n, C_n)$, we have $2 \mid C_{mn}$, and since $\tilde{Q}_{mn}$ is an integer, $2 \mid W_{mn}$; thus, $D_n \mid D_{mn}$.

If $\gamma > 1$, then $4 \mid C_n$ and $4 \mid W_n - 6R^n$. Recall that if $2^\alpha \mid\mid (W_n, C_n)$, then $\alpha = 0$ or 1 by Theorem 4.5. 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

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

so that $2^\gamma \mid W_{mn} - 6R^{mn} \Rightarrow D_n \mid W_{mn} - 6R^{mn} \Rightarrow D_n \mid D_{mn}$. 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.

5.2 The Law of Repetition for $\{D_n\}$

The goal in this section is to develop a law of repetition for $\{D_n\}$.

Suppose $p^\mu \mid\mid D_n$, $\mu \geq 1$ and $p \nmid 6\Delta$. There are three cases to consider.

Case 1. $p^\mu \mid\mid W_n - 6R^n$ and $p^\nu \mid\mid C_n$ such that $\nu > \mu \geq 1$.

Note that $\mu \geq 2$ by Theorem 4.18, and hence $3\mu \geq 2\mu + 2$. We then have $p^{2\nu} \mid F_n$. Thus, by (5.3)

$$W_{pn} \equiv 2R^{pn} L_p(W_n/2R^n) \pmod{p^{2\nu}} \quad \text{and}$$

$$\begin{aligned} L_p(W_n/2R^n) &\equiv 1 + (W_n/2R^n - 1)\left[1 + \left(\frac{p^2-1}{8}\right)(W_n/2R^n + 1)(W_n/2R^n - 3) + \right. \\ &\qquad \left. \frac{(p^2-1)(p^2-9)}{16 \cdot 24}(W_n/2R^n + 1)^2 (W_n/2R^n - 3)^2\right] \pmod{p^{3\mu}}. \end{aligned}$$

Now, since

$$W_n/2R^n + 1 \equiv 4 \pmod{p^\mu} \quad \text{and} \quad p^{2\mu} \mid (W_n/2R^n - 3)^2,$$

we have

$$(W_n/2R^n + 1)^2(W_n/2R^n - 3)^2 \equiv 16(W_n/2R^n - 3)^2 \pmod{p^{3\mu}}.$$

Thus

$$\begin{aligned} L_p(W_n/2R^n) &\equiv 1 + (W_n/2R^n - 1)\left[1 + \left(\frac{p^2-1}{8}\right)(W_n/2R^n + 1)(W_n/2R^n - 3) + \right. \\ &\qquad \left. \frac{(p^2-1)(p^2-9)}{24}(W_n/2R^n - 3)^2\right] \\ &\equiv W_n/2R^n + \left(\frac{p^2-1}{8}\right)((W_n/2R^n)^2 - 1)(W_n/2R^n - 3) + \\ &\qquad \frac{(p^2-1)(p^2-9)}{24}(W_n/2R^n - 1)(W_n/2R^n - 3)^2 \pmod{p^{3\mu}}. \end{aligned}$$

Now

$$W_n/2R^n - 1 \equiv 2 \pmod{p^\mu} \quad \text{and } p^{2\mu} \mid (W_n/2R^n - 3)^2$$

so

$$(W_n/2R^n - 1)(W_n/2R^n - 3)^2 \equiv 2(W_n/2R^n - 3)^2 \pmod{p^{3\mu}}.$$

Thus,

$$\begin{aligned} L_p(W_n/2R^n) &\equiv W_n/2R^n + \left(\frac{p^2-1}{8}\right)((W_n/2R^n)^2 - 1)(W_n/2R^n - 3) + \\ &\qquad \frac{(p^2-1)(p^2-9)}{12}(W_n/2R^n - 3)^2 \pmod{p^{3\mu}}. \end{aligned}$$

Also, we have

$$(W_n/2R^n - 3)^2 \equiv 0 \pmod{p^{2\mu}} \Rightarrow (W_n/2R^n)^2 - 6W_n/2R^n + 9 \equiv 0 \pmod{p^{2\mu}}$$

$$\Rightarrow (W_n/2R^n)^2 - 1 \equiv 6W_n/2R^n - 10 \pmod{p^{2\mu}}.$$

Note, then, that

$$((W_n/2R^n)^2 - 1)(W_n/2R^n - 3) \equiv (6W_n/2R^n - 10)(W_n/2R^n - 3) \pmod{p^{3\mu}}.$$

This yields

$$\begin{aligned} L_p(W_n/2R^n) &\equiv W_n/2R^n + \left(\frac{p^2-1}{8}\right)(6W_n/2R^n - 10)(W_n/2R^n - 3) + \\ &\qquad \frac{(p^2-1)(p^2-9)}{12}(W_n/2R^n - 3)^2 \\ &\equiv \left[(W_n/2R^n - 3) + \left(\frac{p^2-1}{8}\right)(6W_n/2R^n - 10)(W_n/2R^n - 3) + \right. \\ &\qquad \left. \frac{(p^2-1)(p^2-9)}{12}(W_n/2R^n - 3)^2\right] + 3 \pmod{p^{3\mu}}. \end{aligned}$$

This can be rewritten as

$$\begin{aligned} L_p(W_n/2R^n) - 3 &\equiv (W_n/2R^n - 3)\left[1 + \frac{(p^2-1)}{4}(3W_n/2R^n - 9 + 4) + \right. \\ &\qquad \left. \frac{(p^2-1)(p^2-9)}{12}(W_n/2R^n - 3)\right] \\ &\equiv (W_n/2R^n - 3)\left[1 + 3\frac{(p^2-1)}{4}(W_n/2R^n - 3) + 4\frac{(p^2-1)}{4} + \right. \\ &\qquad \left. \frac{(p^2-1)}{4}\frac{(p^2-9)}{3}(W_n/2R^n - 3)\right] \\ &\equiv p^2(W_n/2R^n - 3) + (W_n/2R^n - 3)^2\left[3\frac{(p^2-1)}{4} + \frac{(p^2-1)}{4}\frac{(p^2-9)}{3}\right] \\ &\equiv p^2(W_n/2R^n - 3) + \frac{(p^2-1)}{4}(W_n/2R^n - 3)^2\left[3 + \frac{(p^2-9)}{3}\right] \\ &\equiv p^2(W_n/2R^n - 3) + p^2\frac{(p^2-1)}{12}(W_n/2R^n - 3)^2 \pmod{p^{3\mu}} \\ &\equiv p^2(W_n/2R^n - 3) \pmod{p^{2\mu+2}}. \end{aligned}$$

Observe that

$$W_{pn} - 6R^{pn} \equiv 2R^{pn}L_p(W_n/2R^n) - 6R^{pn} \pmod{p^{2\nu}}$$

and that $\nu > \mu \Rightarrow \nu \geq \mu + 1 \Rightarrow 2\nu \geq 2\mu + 2$. So

$$\begin{aligned} W_{pn} - 6R^{pn} &\equiv 2R^{pn}\left[p^2(W_n/2R^n - 3) + p^2\frac{(p^2-1)}{12}(W_n/2R^n - 3)^2\right] \pmod{p^{2\mu+2}} \\ &\equiv 2R^{pn}\left[p^2(W_n/2R^n - 3)\right] \pmod{p^{2\mu+2}} \\ &\equiv (R^n)^{p-1}p^2(W_n - 6R^n) \pmod{p^{2\mu+2}} \\ &\equiv (1+kp)p^2(W_n - 6R^n) \pmod{p^{2\mu+2}}, \end{aligned}$$

for some $k \in \mathbb{Z}$. Since $p^\mu \mid\mid W_n - 6R^n$ and $2\mu+2 > \mu+2$ we have $p^{\mu+2} \mid\mid W_{pn} - 6R^{pn}$. We also know that $p^{\mu+3} \mid C_{pn}$; hence, $p^{\mu+2} \mid\mid D_{pn}$.

Case 2. $p^\mu \mid\mid W_n - 6R^n$ and $p^\mu \mid\mid C_n$.

We then have $p^{2\mu} \mid F_n$ which gives us

$$W_{pn} \equiv 2R^{pn}L_p(W_n/2R^n) \pmod{p^{2\mu}} \quad \text{and}$$

$$\begin{aligned} L_p(W_n/2R^n) &\equiv 1 + (W_n/2R^n - 1)\left[1 + \binom{(p+1)/2}{2}(W_n/2R^n + 1)(W_n/2R^n - 3)\right] \\ &\equiv W_n/2R^n + \frac{(p^2-1)}{8}((W_n/2R^n)^2 - 1)(W_n/2R^n - 3) \pmod{p^{2\mu}}. \end{aligned}$$

Now, note that since

$$W_n/2R^n + 1 \equiv 4 \pmod{p^\mu} \quad \text{and} \quad W_n/2R^n - 1 \equiv 2 \pmod{p^\mu},$$

we have

$$((W_n/2R^n)^2 - 1) \equiv (W_n/2R^n - 1)(W_n/2R^n + 1) \equiv 8 \pmod{p^\mu}.$$

Together with the fact that $p^\mu \mid W_n/2R^n - 3$, we see that

$$((W_n/2R^n)^2 - 1)(W_n/2R^n - 3) \equiv 8(W_n/2R^n - 3) \pmod{p^{2\mu}}.$$

So

$$L_p(W_n/2R^n) \equiv W_n/2R^n + (p^2-1)(W_n/2R^n - 3) \pmod{p^{2\mu}}.$$

Thus

$$\begin{aligned} W_{pn} - 6R^{pn} &\equiv 2R^{pn}\left[W_n/2R^n + (p^2-1)(W_n/2R^n - 3)\right] - 6R^{pn} \\ &\equiv R^{n(p-1)}\left[W_n + (p^2-1)(W_n - 6R^n) - 6R^n\right] \\ &\equiv p^2(W_n - 6R^n) \pmod{p^{2\mu}}. \end{aligned}$$

Since by Theorem 4.18, $\mu \geq 3$, we get $2\mu \geq \mu + 3$ and we can write

$$W_{pn} - 6R^{pn} \equiv p^2(W_n - 6R^n) \pmod{p^{\mu+3}}.$$

Using the fact $p^\mu \mid\mid W_n - 6R^n$, we get $p^{\mu+2} \mid\mid W_{pn} - 6R^{pn}$. Again we know that $p^{\mu+3} \mid\mid C_{pn} \Rightarrow p^{\mu+2} \mid\mid D_{pn}$.

Case 3. $p^\nu \mid\mid C_n$ and $p^\mu \mid\mid W_n - 6R^n$ such that $\nu < \mu$.

In this case $p^{\nu+3} \mid\mid C_{pn}$ and

$$\begin{aligned} W_{pn} - 6R^{pn} &\equiv p^2(W_n - 6R^n) \pmod{p^{2\nu}} \\ &\equiv p^2(W_n - 6R^n) \equiv 0 \pmod{p^{\nu+3}}. \end{aligned}$$

Thus $p^{\nu+3} \mid W_{pn} - 6R^{pn} \Rightarrow p^{\nu+3} \mid\mid D_{pn}$.

If $p > 3$, $p \mid \Delta$, $p^\mu \mid\mid W_n - 6R^n$ and $p^\nu \mid\mid C_n$ such that $\nu \geq \mu$, we have $p^{2\nu+1} \mid F_n$. Since

$$\tilde{Q}_n^{\lambda_2} V_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) \equiv 2(\tilde{P}_n/2)^{\lambda_1+\lambda_2} \pmod{2^{2\nu+1}}$$

and $p \mid \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!}$ except for $\lambda_1 = p$ we find, by using the reasoning in Section 4.4, that

$$W_{pn} \equiv 2R^{pn}\left[L_p(W_n/2R^n) - (W_n/2R^n)^p\right] + V_p(\tilde{P}_n, \tilde{Q}_n) \pmod{p^{2\nu+2}}.$$

We may use the fact that

$$\begin{aligned} V_p(\tilde{P}_n, \tilde{Q}_n) &\equiv \tilde{P}_n(\tilde{P}_n/2)^{p-1} + \tilde{P}_n^{p-2}\tilde{\Delta}_n\binom{p}{2} \pmod{p^{2\nu+2}} \\ &\equiv \tilde{P}_n(\tilde{P}_n/2)^{p-1} \pmod{p^{2\nu+2}} \end{aligned}$$

to get

$$\begin{aligned} W_{pn} &\equiv 2R^{pn}L_p(W_n/2R^n) - 2R^{pn}(W_n/2R^n)^p + W_n(W_n/2)^{p-1} \\ &\equiv 2R^{pn}L_p(W_n/2R^n) \pmod{p^{2\nu+2}}. \end{aligned}$$

Since

$$W_{pn} - 6R^{pn} \equiv p^2R^{(p-1)n}(W_n - 6R^n) \pmod{p^{2\mu+2}},$$

we get $p^{\mu+2} \mid\mid D_{pn}$ when $\nu \geq \mu (\geq 1)$.

If $\nu < \mu$, then $p^{\nu+3} \mid W_{pn} - 6R^{pn}$ and $p^{\nu+3} \mid\mid D_{pn}$.

If $p = 3$, $3^{\mu} \mid\mid D_n$, $3^{\mu} \mid\mid W_n - 6R^n$ and $3^{\nu} \mid\mid C_n$ where $\nu \geq \mu$, then we use

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

We have $3^{2\nu+1} \mid 3\Delta C_n^2$ and

$$4(W_{3n} - 6R^{3n}) \equiv W_n^2(W_n - 6R^n) \pmod{3^{2\nu+1}}.$$

Suppose $\mu > 1$. Since $\nu \geq \mu \geq 2 \Rightarrow 2\nu + 1 \geq \mu + 3$ we have

$$4(W_{3n} - 6R^{3n}) \equiv W_n^2(W_n - 6R^n) \pmod{3^{\mu+3}}.$$

Since $(D_n, R) \mid 2$, and $9 \mid W_n - 6R^n$, we must have $3 \mid\mid W_n$. Thus for $\mu > 1$ we have $3^{\mu+2} \mid\mid D_{3n}$. If $\mu = 1$, all we can say is that $3^{\mu+2} \mid D_{3n}$.

Now if $p = 3$, $\mu > 1$, $3^\mu \mid\mid C_n$ and $3^\nu \mid\mid W_n - 6R^n$ such that $\nu > \mu$, we have that $3^{\mu+3} \mid\mid C_{3n}$ and

$$\begin{aligned} 4(W_{3n} - 6R^{3n}) &\equiv W_n^2(W_n - 6R^n) \pmod{3^{2\mu+1}} \\ &\equiv W_n^2(W_n - 6R^n) \pmod{3^{\mu+3}} \\ &\equiv 0 \pmod{3^{\mu+3}}, \end{aligned}$$

hence $3^{\mu+3} \mid\mid D_{3n}$. If $\mu = 1$, we can only say that $3^{\mu+3} \mid D_{3n}$.

For the case where $p = 2$ and $2 \nmid R$ we have the following. If $2 \mid D_n$, then $2 \mid W_n$ and $2 \mid C_n$, hence $2 \mid C_{2n}/C_n$ as $C_{2n} = C_n(W_n + 2R^n)$. Also, since $\tilde{Q}_n = (W_n^2 - \Delta C_n^2)/4$ is odd in this case, we get $W_n^2 - \Delta C_n^2 \equiv 4 \pmod 8$ and

$$W_n^2 + \Delta C_n^2 \equiv 4 + 2\Delta C_n^2 \equiv 4 \pmod 8.$$

Now

$$2W_{2n} = \Delta C_n^2 + W_n^2 - 4R^n W_n \equiv \Delta C_n^2 + W_n^2 \equiv 4 \pmod 8.$$

This means

$$W_{2n} \equiv 2 \pmod 4 \Rightarrow 2 \mid\mid W_n \Rightarrow 4 \mid W_{2n} - 6R^{2n}.$$

Now suppose further that $2^m \mid D_n$ and $m \geq 2$. So then

$$2^{2m} \mid (W_n - 6R^n)^2 \Rightarrow W_n^2 \equiv 12R^n W_n - 36R^{2n} \pmod{2^{2m}}.$$

This, together with the identity $2W_{2n} = \Delta C_n^2 + W_n^2 - 4R^n W_n$ yields,

$$2W_{2n} \equiv -36R^{2n} + 12R^n W_n - 4R^n W_n \equiv 8R^n W_n - 36R^{2n} \pmod{2^{2m}}.$$

So then

$$\begin{aligned} 2(W_{2n} - 6R^{2n}) &\equiv 8R^n W_n - 36R^{2n} - 12R^{2n} \pmod{2^{2m}} \\ &\equiv 8R^n W_n - 48R^{2n} \pmod{2^{2m}} \\ &\equiv 8R^n(W_n - 6R^n) \pmod{2^{2m}}. \end{aligned}$$

Hence,

$$W_{2n} - 6R^{2n} \equiv 4R^n(W_n - 6R^n) \pmod{2^{2m-1}},$$

and since $m \geq 2$, we get $2m - 1 \geq m + 1$, so

$$W_{2n} - 6R^{2n} \equiv 4R^n(W_n - 6R^n) \pmod{2^{m+1}}.$$

Thus we can see $2^{m+1} \mid W_{2n} - 6R^{2n}$. Thus, if $2^m \mid D_n$, then $2^{m+1} \mid D_{2n}$.

When $m \geq 4$ we can say more. Here we have $16 \mid W_n - 6R^n$, so $2 \nmid R$, since otherwise $4 \mid (W_n, C_n)$ and this is a contradiction because $(W_n, C_n) \mid 2$ when $(Q, R) = 1$ by Theorem 4.5. Now

$$W_n + 2R^n = W_n - 6R^n + 8R^n \Rightarrow 8 \mid\mid W_n + 2R^n \Rightarrow 8 \mid\mid C_{2n}/C_n.$$

Also, if $2^\nu \mid\mid C_n$, then

$$2W_{2n} \equiv W_n^2 - 4R^n W_n \pmod{2^{2\nu}},$$

or

$$2(W_{2n} - 6R^{2n}) \equiv (W_n - 6R^n)^2 + 8R^n(W_n - 6R^n) \pmod{2^{2\nu}}.$$

Now let $2^\mu \mid\mid W_n - 6R^n$.

Case 1. If $\nu \geq \mu$, we get

$$2(W_{2n} - 6R^{2n}) \equiv 8R^n(W_n - 6R^n) \pmod{2^{2\mu}}.$$

Hence

$$W_{2n} - 6R^{2n} \equiv 4R^n(W_n - 6R^n) \pmod{2^{2\mu-1}}.$$

Now we use the fact $\mu \geq 4$ to see that

$$W_{2n} - 6R^{2n} \equiv 4R^n(W_n - 6R^n) \pmod{2^{\mu+3}}.$$

Hence $2^{\mu+2} \mid\mid W_{2n} - 6R^{2n}$ and $2^{\nu+3} \mid\mid C_{2n} \Rightarrow 2^{m+2} \mid\mid D_{2n} \Rightarrow 4 \mid\mid D_{2n}/D_n$ when $m = \mu$. Thus by induction we get $2^{2k} \mid\mid D_{2^k n}/D_n$.

Case 2. If $\nu < \mu$, then we have $2^{\nu+3} \mid W_{2n} - 6R^{2n}$ and $2^{\nu+3} \mid\mid C_{2n} \Rightarrow 2^{\nu+3} \mid\mid D_{2n} \Rightarrow 2^3 \mid\mid D_{2n}/D_n$. However, since we do not know that $2^{\nu+4} \mid W_{2n} - 6R^{2n}$, the best we can say in general is that, if $2^\gamma \mid\mid D_{2^k n}/D_n$, then $\gamma \leq 3k$.

Theorem 5.1. *If p is a prime, $p^\lambda \mid\mid D_n$ $(\lambda \geq 1)$ and $p \nmid m$, then $p^\lambda \mid\mid D_{mn}$.*

Proof. Suppose first that $p \neq 2$. If $2 \nmid m$, then since $p \mid D_n$, we get

$$\begin{aligned}
\frac{C_{mn}}{C_n} &\equiv mR^{n(m-1)} + m\left(\frac{m^2-1}{8}\right)\frac{R^{n(m-3)}}{4}(W_n - 2R^n)(W_n + 2R^n) \pmod{p} \\
&\equiv mR^{n(m-1)} + m\left(\frac{m^2-1}{8}\right)\frac{R^{n(m-3)}}{4}32R^{2n} \pmod{p} \\
&\equiv m^3R^{n(m-1)} \pmod{p}.
\end{aligned}$$

If $2 \mid m$, then

$$\begin{aligned}
\frac{C_{mn}}{C_n} &\equiv m\left(\frac{m}{m/2-1}\binom{m/2}{2}\frac{R^{n(m-2)}}{2}(W_n + 2R^n)\right) \pmod{p} \\
&\equiv m\left(\left(\frac{m}{m/2-1}\right)\left(\frac{(m/2)(m/2-1)}{2}\right)\frac{R^{n(m-2)}}{2}8R^n\right) \pmod{p} \\
&\equiv m^3R^{n(m-1)} \pmod{p}.
\end{aligned}$$

Suppose $p^\lambda \mid\mid D_n$. There two cases: either $p^\lambda \mid\mid C_n$ or $p^\lambda \mid\mid W_n - 6R^n$. If $p^\lambda \mid\mid C_n$ and $p \nmid m$, then $p^{\lambda+1} \nmid C_{mn}$, and we have $p^\lambda \mid\mid D_{mn}$.

On the other hand, if $p^\lambda \mid\mid W_n - 6R^n$, then $p^\lambda \mid C_n$ and $p^{2\lambda} \mid F_n$. If $2 \nmid m$,

$$\begin{aligned} L_m(W_n/2R^n) &\equiv 1 + (W_n/2R^n - 1) + \left(\frac{m^2-1}{8}\right)(W_n/2R^n - 1)(W_n/2R^n + 1) \\ &\qquad\qquad (W_n/2R^n - 3) \pmod{p^{2\lambda}} \\ &\equiv W_n/2R^n + \left(\frac{m^2-1}{8}\right) 8(W_n/2R^n - 3) \pmod{p^{2\lambda}} \\ &\equiv W_n/2r^n + m^2(W_n/2R^n - 3) - (W_n/2R^n - 3) \pmod{p^{2\lambda}} \\ &\equiv m^2(W_n/2R^n - 3) + 3 \pmod{p^{\lambda+1}}. \end{aligned}$$

If $2 \mid m$ we get

$$\begin{aligned} L_m(W_n/2R^n) &\equiv 1 + \frac{m}{m/2} + \frac{m}{m/2-1}\binom{m/2}{2}(W_n/2R^n + 1)(W_n/2R^n - 3) \pmod{p^{2\lambda}} \\ &\equiv 3 + \left(\frac{m}{m/2-1}\right)\left(\frac{m/2(m/2-1)}{2}\right) 4(W_n/2R^n - 3) \pmod{p^{2\lambda}} \\ &\equiv m^2(W_n/2R^n - 3) + 3 \pmod{p^{\lambda+1}}. \end{aligned}$$

We can then see

$$\begin{aligned} W_{mn} - 6R^{mn} &\equiv 2R^{mn} L_m(W_n/2R^n) - 6R^{mn} \pmod{p^{\lambda+1}} \\ &\equiv 2R^{mn}\left(L_m(W_n/2R^n) - 3\right) \pmod{p^{\lambda+1}} \\ &\equiv 2R^{mn}\left(m^2(W_n/2R^n - 3)\right) \pmod{p^{\lambda+1}}. \end{aligned}$$

But then $p^{\lambda+1} \mid W_{mn} - 6R^{mn} \Rightarrow p \mid m$. Hence if $p \nmid m$ and $p^\lambda \mid\mid D_n$, then $p^\lambda \mid\mid D_{mn}$.

Now for the case of $p = 2$. Since $2 \mid D_n$, we have $2 \mid C_n$ and $2 \mid W_n$. This means that $2 \mid \tilde{P}_n$ and $2 \nmid \tilde{Q}_n$ by Theorem 4.5. By Theorem 4.10, we have

$$C_{mn}/C_n \equiv m \pmod{2}.$$

Thus, if $2 \nmid m$, then $2 \nmid C_{mn}/C_n$. If $2^\lambda \mid\mid C_n$, then $2^{\lambda+1} \nmid C_{mn}$ and so $2^{\lambda+1} \nmid D_{mn}$

when $2 \nmid m$. If $2^{\lambda+1} \mid C_n$, then $2^{\lambda} \mid\mid W_n - 6R^n$. In this case $2^{2\lambda} \mid F_n$. If $2 \nmid m$, then

$$\begin{aligned} W_{mn} &\equiv 2R^{mn} L_m(W_n/2R^n) \pmod{2^{2\lambda}} \\ &\equiv 2R^{mn}(m^2(W_n/2R^n - 3) + 3) \pmod{2^{\lambda+1}}. \end{aligned}$$

Thus

$$\begin{aligned} W_{mn} - 6R^{mn} &\equiv 2m^2 R^{mn}(W_n/2R^n - 3) \pmod{2^{\lambda+1}} \\ &\equiv m^2 R^{m(n-1)}(W_n - 6R^n) \pmod{2^{\lambda+1}}. \end{aligned}$$

Since $2^{\lambda} \mid\mid W_n - 6R^n$, we get $2^{\lambda} \mid\mid W_{mn} - 6R^{mn}$ when m is odd. Hence $2^{\lambda+1} \nmid D_{mn}$ when $2 \nmid m$.

Thus, we have shown that if p is any prime and $p^{\lambda} \mid\mid D_n$, then $p^{\lambda} \mid\mid D_{mn}$ when $p \nmid m$. □

Our *Law of Repetition* for $\{D_n\}$ is stated in the following theorem.

Theorem 5.2. *If* $p^{\lambda} \mid\mid D_n$ $(p \neq 2, p^{\lambda} \neq 3)$, *then*

$$\begin{aligned} &p^{\lambda+2} \mid\mid D_{pn} \quad \textit{when} \quad p^{\lambda} \mid\mid W_n - 6R^n \quad \textit{and} \\ &p^{\lambda+3} \mid\mid D_{pn} \quad \textit{otherwise}\ . \end{aligned}$$

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 $p \neq 2$, 3 and $p^{\lambda} \mid\mid W_n - 6R^n$, $p^{\lambda} \mid\mid D_n$, 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. We have given some reason in Chapter 4 to believe that 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 as complete a 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, then, 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.

5.3 The Law of Apparition for $\{D_n\}$

Definition 5.3. *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 towards a result very comparable to Theorem 2.4. 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.

Lemma 5.4. *Suppose p is a prime, $p \nmid 2R\Delta$ and $\mathbb{K}$ is the splitting field of $f(x)$ in $\mathbb{F}_p[x]$. If α, β, γ are the zeros of $f(x)$ in $\mathbb{K}$, then $p \mid D_n$ if and only if $\alpha^n = \beta^n = \gamma^n$ in $\mathbb{K}$.*

Proof. ($\Rightarrow$) If $p \mid D_n$, then $p \mid C_n$ and we may assume with no loss of generality that $\alpha^n = \beta^n$. Since

$$W_n - 6R^n = 2\beta^n(\alpha^n - \gamma^n)^2 - (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\alpha^n + \gamma^n),$$

it follows that

$$2\beta^n(\alpha^n - \gamma^n)^2 \equiv (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\alpha^n + \gamma^n) \pmod{p},$$

as $p \mid W_n - 6R^n$ and hence $\alpha^n = \gamma^n$.

($\Leftarrow$)On the other hand, if $\alpha^n = \beta^n = \gamma^n$, then it is clear that $p \mid D_n$. □

We are now able to present an important result concerning $\omega(p)$.

Theorem 5.5. *Suppose p is a prime such that $p \nmid 2R\Delta$ and suppose further that $\omega = \omega(p)$ exists for $\{D_n\}$. If $p \mid D_n$, then $\omega \mid n$.*

Proof. Since $p \mid D_n$ and $p \mid D_\omega$ we have $\alpha^n = \beta^n = \gamma^n$ and $\alpha^\omega = \beta^\omega = \gamma^\omega$ in $\mathbb{K}$ by Lemma 5.4. If $\omega \nmid n$, then $n = \omega q + r$, where $0 < r < \omega$. By Lemma 4.23, we get $\alpha^r = \beta^r = \gamma^r$ and $p \mid D_r$ by Lemma 5.4. Since this contradicts the definition of ω, we must have $r = 0$ and $\omega \mid n$. □

We next note that if $p \mid R$ and $p \neq 2$, then $\omega(n)$ does not exist. If $2 \mid R$, then $2 \nmid Q$. By our results in Theorem 4.15, there exists a rank of apparition r for $\{C_n\}$ of 2. Since $2 \mid C_n \Rightarrow 2 \mid W_n$, we see that $\omega = \omega(2) = r$ and $2 \mid D_n$ if and only if $r \mid n$.

Theorem 5.6. *If $p \nmid R$, then $\omega(p)$ must exist. Further, if $p \mid D_n$, then $\omega(p) \mid n$.*

Proof. We have already seen that this holds if $p = 2$. We now turn our attention to the case of $p = 3$. If $3 \mid C_n$, then by Corollary 3.10.1 we have

$$\begin{aligned}
8W_{4n} &\equiv 4W_{2n}^2 - 16R^{2n}W_{2n} \pmod 3 \\
&\equiv 2W_{2n}(2W_{2n} - 8R^{2n}) \pmod 3 \\
&\equiv (W_n^2 - 4R^nW_n)((W_n^2 - 4R^nW_n - 8R^{2n}) \pmod 3 \\
&\equiv W_n(W_n - R^n)((W_n^2 + 2R^nW_n + R^{2n}) \pmod 3 \\
&\equiv W_n(W_n - R^n)(W_n + R^n)^2 \pmod 3 \\
&\equiv 0 \pmod 3,
\end{aligned}$$

since $3 \nmid R$, then 3 must divide one of W_n, $W_n - R^n$ or $W_n + R^n$. Thus, since $r(3)$ exists and is unique when $3 \nmid \Delta$, we see by Table 4.1 that $\omega(3)$ exists. By Theorem 5.5, we also see that $\omega(3) \mid n$ if $p \mid D_n$. If $p \nmid 6\Delta R$, then p is either an S prime, I prime or Q prime. If p is an I prime, then $\alpha^p = \beta$, $\beta^p = \gamma$, $\gamma^p = \alpha$ in $\mathbb{F}_{p^3}$, the

splitting field of $f(x)$. Hence

$$\alpha^{p^2+p+1} = \beta^{p^2+p+1} = \gamma^{p^2+p+1} = R$$

and $p \mid D_{p^2+p+1}$.

If p is an S prime, then $\alpha^{p-1} = \beta^{p-1} = \gamma^{p-1} = 1$ in the splitting field $\mathbb{F}_p$ of $f(x)$. Hence, $p \mid D_{p-1}$ by Lemma 5.4.

If p is a Q prime, then $\alpha^{p^2-1} = 1$, $\beta^{p^2-1} = (\beta^{p+1})^{p-1} = (\gamma\beta)^{p-1} = (R/\alpha)^{p-1} = 1$, $\gamma^{p^2-1} = 1$ and $p \mid D_{p^2-1}$. Thus, if $p \nmid 6\Delta R$, then $\omega(p)$ exists, and if $p \mid D_n$, then $\omega(p) \mid n$ by Theorem 5.5.

When $p \mid \Delta$ and $p \neq 2$, we have seen that there are two cases:

Case 1. $p \mid P^2 - 3Q$.

In this case, we have seen in Section 4.3 that there is a unique $r = r(p) = p$, and $p \mid C_n$ if and only if $r \mid n$. Also, since, in this case, $p \mid W_n - 6R^n$ whenever $p \mid C_n$, we have $\omega = r$ and $\omega \mid n$ if $p \mid D_n$.

Case 2. $p \nmid P^2 - 3Q$.

In this case, we know that by our results in Section 4.3 that $p \mid D_n$ if and only if $r \mid n$. Here r is the least positive integer such that $p \mid a^r - b^r$, where a, b are as in equation (4.12). Thus $\omega(p) = r$ and $r \mid p - 1$. Note that in both cases $p \mid D_n \Rightarrow \omega(p) \mid n$.

Thus if $p \nmid R$, we have shown that $\omega(p)$ always exists and $\omega(p) \mid n$ whenever $p \mid D_n$. □

Corollary 5.6.1. *If p is a prime and $\omega(p)$ exists, then $\omega(p) \leq p^2 + p + 1$.*

If p is an I prime, we have a very simple result connecting divisibility of C_n and D_n by p.

Theorem 5.7. *If p is an I prime, then $p \mid C_n \Leftrightarrow p \mid D_n$.*

Proof. Clearly, if $p \mid D_n$, then $p \mid C_n$. Let α, β, γ be the zeros of $f(x)$ in $\mathbb{K} = \mathbb{F}_{p^3}$. In $\mathbb{K}$ we must have $\alpha^n = \beta^n \Rightarrow \alpha^{pn} = \beta^{pn} \Rightarrow \beta^n = \gamma^n \Rightarrow \alpha^n = \beta^n = \gamma^n$. It follows that $W_n = 6\alpha^n\beta^n\gamma^n = 6R^n$ in $\mathbb{K}$. Thus, $p \mid W_n - 6R^n \Rightarrow p \mid D_n$. □

Since for any Q prime p we know that $p \mid C_{p+1}$, it is of some interest to determine under what conditions $p \mid D_{p+1}$. We require a simple lemma.

Lemma 5.8. *Let α, β, γ be the zeros of $f(x)$ in $\mathbb{F}_{p^2}$ where $\alpha^p = \alpha$, $\beta^p = \gamma$, $\gamma^p = \beta$. If $p \mid Q^3 - RP^3$, then $\alpha^3 = R$ in $\mathbb{F}_{p^2}$.*

Proof. Suppose $p \mid Q^3 - RP^3$. If $p \mid P$, then $p \mid Q$ and $f(x) \equiv x^3 - R \pmod{p}$; hence, $\alpha^3 = R$ in $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$. If $p \nmid P$, then

$$f(x) \equiv x^3 - Px^2 + Qx - (Q/P)^3 \pmod{p}$$

and

$$P^3 f(x) \equiv (Px - Q)(P^2x^2 + (PQ - P^3)x + Q^2) \pmod{p}.$$

Because β, $\gamma \notin \mathbb{F}_p$ it follows that $P\alpha - Q = 0$ in $\mathbb{F}_p$; hence,

$$\alpha^3 = Q^3/P^3 = R \quad \text{in} \quad \mathbb{F}_{p^2}.$$

□

We are now able to show that for a fixed triple P, Q, R, there can only be a finite number of Q primes such that $p \mid D_{p+1}$.

Theorem 5.9. *If p is a Q prime, then $p \mid D_{p+1}$ if and only if $p \mid Q^3 - RP^3$.*

Proof. Since p is a Q prime by Corollary 4.24.1, we have $p \mid C_{p+1}$. In $\mathbb{F}_{p^2}$, we have

$$W_{p+1} = 2R^2 + 2(\beta\gamma)^3 + 2R\alpha^3;$$

hence, since $\alpha \neq 0$ ($R \neq 0$), we have

$$\begin{aligned} W_{p+1} - 6R^{p+1} &= 2(\beta\gamma)^3 + 2R\alpha^3 - 4R^2 \\ &= 2((R/\alpha)^3 + R\alpha^3 - 2R^2) \\ &= \frac{2R}{\alpha^3}(\alpha^3 - R)^2. \end{aligned}$$

It follows that $p \mid W_{p+1} - 6R^{p+1}$ if and only if $\alpha^3 = R$ in $\mathbb{F}_{p^2}$. By Lemma 5.8 we know that if $p \mid Q^3 - RP^3$, then $\alpha^3 = R$. If $\alpha^3 = R$, then since $\alpha^3 - P\alpha^2 + Q\alpha - R = 0$, we get $P\alpha^2 - Q\alpha = 0$ and hence $P\alpha - Q = 0$. If $P = 0$ in $\mathbb{F}_{p^2}$, then $p \mid Q^3 - RP^3$. If $P \neq 0$, then $\alpha = Q/P$ and $R = (Q/P)^3 \Rightarrow p \mid Q^3 - RP^3$. □

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

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

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

Theorem 5.10. *If $p \nmid R$, $p^\alpha \mid D_n$, 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 $p^\gamma \mid\mid m$ and put $m = m'p^\gamma$ ($p \nmid m'$). Since $p^\alpha \nmid D_{p^{\nu-1}\omega(p)}$ we must have $p^\alpha \nmid D_{m'p^{\nu-1}\omega(p)} \Rightarrow \gamma > \nu - 1$. But $p^\alpha \mid D_{m'p^\nu\omega(p)} \Rightarrow \gamma = \nu$.

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

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 2.4.1. Again, as seen in Chapter 4, this is another result that did not hold for $\{C_n\}$.

Theorem 5.12.

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

Proof. Since D_n is a divisibility sequence we have $D_{(m,n)} \mid D_n$, $D_{(m,n)} \mid D_m \Rightarrow D_{(m,n)} \mid (D_n, D_m)$. Let $p^\alpha \mid\mid (D_n, D_m)$, then $\omega(p^\alpha)$ exists and $\omega(p^\alpha) \mid n$, $\omega(p^\alpha) \mid m$ hence $\omega(p^\alpha) \mid (m, n) \Rightarrow p^\alpha \mid D_{(m,n)}$. Thus $(D_n, D_m) = D_{(m,n)}$. □

In Chapter 4 we were able to develop a result somewhat akin to Carmichael's result in Theorem 2.5. Surprisingly, if we look at $\{D_n\}$ rather than $\{C_n\}$, we can in fact do better. We have that

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

where F_n is as in (4.11). If $2^\nu \mid\mid C_n$ and $\nu > 1$, then $C_n \mid F_n$ and

$$\frac{C_{mn}}{C_n} \equiv m^3 R^{n(m-1)} \pmod{D_n}. \tag{5.4}$$

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

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

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

If $(D_n, R) = 2$, then by Lemma 4.4, $2 \mid\mid D_n$. We then have $(\frac{C_{mn}}{C_n}, D_n/2) \mid m^3$. Since $(D_n/2, R) = 1$ and $(\frac{C_{mn}}{C_n}, 2) \mid m$ we have $(\frac{C_{mn}}{C_n}, D_n) \mid m^3$.

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

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

We first observe that if $p \nmid m$, then $p \nmid D_{mn}/D_n$, which is a contradiction to Theorem 5.1, 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 $\gamma = \lambda - \nu \leq 3\mu \Rightarrow p^\gamma \mid m^3$. We now have the desired analogue of Theorem 2.5.

Theorem 5.13. *If m, $n \geq 1$, then*

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

The next two theorems will be needed in Chapter 6 to produce an analogue to Euler's criterion for the Lucas functions.

Theorem 5.14. *Let p be an I prime and $p \equiv 1 \pmod 3$, then*

$$C_{\frac{p^2+p+1}{3}} \equiv 0 \pmod p \quad \textit{and} \quad W_{\frac{p^2+p+1}{3}} \equiv 6R^{\frac{p^2+p+1}{3}} \pmod p$$

if and only if $R^{\frac{p-1}{3}} \equiv 1 \pmod p$.

Proof. We have α, β, γ as the zeros of $f(x)$ in $\mathbb{F}_{p^3}$ where $\beta = \alpha^p$, $\gamma = \beta^p$. In $\mathbb{F}_{p^3}$ we get $R = \alpha^{p^2+p+1}$ and

$$R^{\frac{p-1}{3}} = (\alpha^{p^2+p+1})^{\frac{p-1}{3}} = \alpha^{\frac{p^3-1}{3}}.$$

Hence

$$\alpha^{\frac{p^2+p+1}{3}} R^{\frac{p-1}{3}} = \alpha^{\frac{p^2+p+1}{3}} \alpha^{\frac{p^3-1}{3}} = \alpha^{\frac{p^2+p+1}{3}+\frac{p^3-1}{3}} = \alpha^{\frac{p^3+p^2+p}{3}} = \alpha^{p(\frac{p^2+p+1}{3})}.$$

This yields

$$\beta^{\frac{p^2+p+1}{3}} = \alpha^{\frac{p^2+p+1}{3}} R^{\frac{p-1}{3}}.$$

Similarly, one may show

$$\gamma^{\frac{p^2+p+1}{3}} = \beta^{\frac{p^2+p+1}{3}} R^{\frac{p-1}{3}} \quad \text{or} \quad \gamma^{\frac{p^2+p+1}{3}} = \alpha^{\frac{p^2+p+1}{3}} R^{\frac{2(p-1)}{3}}.$$

Now if $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$, then $p \mid C_{\frac{p^2+p+1}{3}}$. If $R^{\frac{p-1}{3}} \not\equiv 1 \pmod{p}$, then $p \nmid C_{\frac{p^2+p+1}{3}}$. Then $R^{p-1} = 1$ and

$$\begin{aligned}
\alpha^{\frac{p^2+p+1}{3}} - \beta^{\frac{p^2+p+1}{3}} &= \alpha^{\frac{p^2+p+1}{3}}[1 - R^{\frac{p-1}{3}}], \\
\beta^{\frac{p^2+p+1}{3}} - \gamma^{\frac{p^2+p+1}{3}} &= \alpha^{\frac{p^2+p+1}{3}}[R^{\frac{p-1}{3}} - R^{\frac{2(p-1)}{3}}], \\
\gamma^{\frac{p^2+p+1}{3}} - \alpha^{\frac{p^2+p+1}{3}} &= \alpha^{\frac{p^2+p+1}{3}}[R^{\frac{2(p-1)}{3}} - 1]
\end{aligned}$$

imply

$$\Delta C^2_{\frac{p^2+p+1}{3}} = -27R^2 \neq 0.$$

Now note

$$\begin{aligned} W_{\frac{p^2+p+1}{3}} &= \alpha^{\frac{2(p^2+p+1)}{3}}\beta^{\frac{p^2+p+1}{3}} + \beta^{\frac{2(p^2+p+1)}{3}}\alpha^{\frac{p^2+p+1}{3}} + \beta^{\frac{2(p^2+p+1)}{3}}\gamma^{\frac{p^2+p+1}{3}} + \\ &\quad \gamma^{\frac{2(p^2+p+1)}{3}}\beta^{\frac{p^2+p+1}{3}} + \gamma^{\frac{2(p^2+p+1)}{3}}\alpha^{\frac{p^2+p+1}{3}} + \alpha^{\frac{2(p^2+p+1)}{3}}\gamma^{\frac{p^2+p+1}{3}} \\ &= \alpha^{\frac{2(p^2+p+1)}{3}}\alpha^{\frac{p^2+p+1}{3}}R^{\frac{p-1}{3}} + \alpha^{\frac{2(p^2+p+1)}{3}}\alpha^{\frac{p^2+p+1}{3}}R^{\frac{2(p-1)}{3}} + \\ &\quad \alpha^{\frac{2(p^2+p+1)}{3}}R^{\frac{2(p-1)}{3}}\alpha^{\frac{p^2+p+1}{3}}R^{\frac{2(p-1)}{3}} + \alpha^{\frac{2(p^2+p+1)}{3}}R^{\frac{p-1}{3}}\alpha^{\frac{p^2+p+1}{3}}R^{\frac{p-1}{3}} + \\ &\quad \alpha^{\frac{2(p^2+p+1)}{3}}R^{\frac{p-1}{3}}\alpha^{\frac{p^2+p+1}{3}} + \alpha^{\frac{2(p^2+p+1)}{3}}\alpha^{\frac{p^2+p+1}{3}}R^{\frac{2(p-1)}{3}} \\ &= 3R[R^{\frac{p-1}{3}} + R^{\frac{2(p-1)}{3}}]. \end{aligned}$$

If $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$, then $W_{\frac{P^2+p+1}{3}} - 6R \equiv 0 \pmod{p}$. Also, since $3 \mid p+2$, we have $R^{\frac{(p+2)(p-1)}{3}} \equiv 1 \pmod{p} \Rightarrow R^{\frac{p^2+p+1}{3}} \equiv R \pmod{p}$. Thus if $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$, we get $p \mid W_{\frac{p^2+p+1}{3}} - 6R^{\frac{p^2+p+1}{3}}$. If $R^{\frac{p-1}{3}} \not\equiv 1 \pmod{p}$, then $R^{\frac{2(p-1)}{3}} + R^{\frac{p-1}{3}} \equiv -1 \not\equiv 2 \pmod{p}$ and $p \nmid W_{\frac{p^2+p+1}{3}} - 6R^{\frac{p^2+p+1}{3}}$ as $W_{\frac{p^2+p+1}{3}} \equiv -3R^{\frac{p^2+p+1}{3}} \pmod{p}$. □

Theorem 5.15. *Let p ($\equiv 1 \pmod 3$) be a Q prime, then $p \mid D_{\frac{p^2-1}{3}}$ if and only if $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$.*

Proof. We have α, β, γ as the zeros of $f(x)$ in $\mathbb{F}_{p^2}$ such that

$$\alpha^p = \alpha, \quad \beta^p = \gamma \quad \text{and } \gamma^p = \beta$$

and

$$\alpha^{p-1} = 1, \quad \alpha^{p+1} = \alpha^2, \quad \beta^{p+1} = \beta\gamma \quad \text{and} \quad \gamma^{p+1} = \beta\gamma.$$

Now $\beta\gamma = R/\alpha$ and

$$\begin{aligned} \beta^{\frac{p^2-1}{3}} = \gamma^{\frac{p^2-1}{3}} &= (\beta\gamma)^{\frac{p-1}{3}} = \left(\frac{R}{\alpha}\right)^{\frac{p-1}{3}} = \frac{R^{\frac{p-1}{3}}}{\alpha^{\frac{p-1}{3}}} \cdot \frac{\alpha^{\frac{2(p-1)}{3}}}{\alpha^{\frac{2(p-1)}{3}}} = R^{\frac{p-1}{3}}\alpha^{\frac{2(p-1)}{3}} \\ &= R^{\frac{p-1}{3}}(\alpha^2)^{\frac{p-1}{3}} = R^{\frac{p-1}{3}}(\alpha^{p+1})^{\frac{p-1}{3}} = R^{\frac{p-1}{3}}\alpha^{\frac{p^2-1}{3}}. \end{aligned}$$

We know that $p \mid C_{\frac{p^2-1}{3}}$ and

$$W_{\frac{p^2-1}{3}} \equiv 2\alpha^{p^2-1}(1 + R^{\frac{p-1}{3}} + R^{\frac{2(p-1)}{3}}) \equiv 2(1 + R^{\frac{p-1}{3}} + R^{\frac{2(p-1)}{3}}) \pmod{p}.$$

Hence

$$W_{\frac{p^2-1}{3}} - 6R^{\frac{p^2-1}{3}} \equiv W_{\frac{p^2-1}{3}} - 6R^{\frac{2(p-1)}{3}} \equiv 2\left(1 - R^{\frac{2(p-1)}{3}}\right)^2 \pmod{p}.$$

Thus $p \mid W_{\frac{p^2-1}{3}} - 6R^{\frac{p^2-1}{3}} \Leftrightarrow R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$.

□

A companion result to Theorem 5.15 for $p \equiv -1 \pmod 3$ is given below.

Theorem 5.16. *If p is a Q prime and $p \equiv -1 \pmod 3$, then*

$$p \mid D_{\frac{p^2-1}{3}} \quad \textit{if and only if} \quad p \mid C_{\frac{p+1}{3}}.$$

Proof. If $p \mid C_{\frac{p+1}{3}}$, then

$$\alpha^{\frac{p+1}{3}} = \beta^{\frac{p+1}{3}}, \quad \beta^{\frac{p+1}{3}} = \gamma^{\frac{p+1}{3}} \quad \text{or} \quad \alpha^{\frac{p+1}{3}} = \gamma^{\frac{p+1}{3}}.$$

In the first case, since $\alpha^{\frac{p+1}{3}} \in \mathbb{F}_p$, we get $\beta^{\frac{p^2-1}{3}} = 1 = \alpha^{\frac{p^2-1}{3}}$. In the second case,

$$\beta^{\frac{p^2-1}{3}} = (\beta^{p-1})^{\frac{p+1}{3}} = (\gamma/\beta)^{\frac{p+1}{3}} = 1 = (\beta/\gamma)^{\frac{p+1}{3}} = (\gamma^{p-1})^{\frac{p+1}{3}} = \gamma^{\frac{p^2-1}{3}}.$$

In the third case, since $\alpha^{\frac{p+1}{3}} \in \mathbb{F}_p$, we get $\gamma^{\frac{p^2-1}{3}} = 1 = \alpha^{\frac{p^2-1}{3}}$. Since $(\alpha\beta\gamma)^{\frac{p^2-1}{3}} = 1$, we get $\alpha^{\frac{p^2-1}{3}} = \beta^{\frac{p^2-1}{3}} = \gamma^{\frac{p^2-1}{3}}$ in all of the three cases. It follows that $p \mid C_{\frac{p^2-1}{3}}$ and $p \mid W_{\frac{p^2-1}{3}} - 6R^{\frac{p^2-1}{3}}$.

Conversely, if $p \mid D_{\frac{p^2-1}{3}}$, then

$$1 = \alpha^{\frac{p^2-1}{3}} = \beta^{\frac{p^2-1}{3}}, \quad \beta^{\frac{p^2-1}{3}} = \gamma^{\frac{p^2-1}{3}} \quad \text{or} \quad 1 = \alpha^{\frac{p^2-1}{3}} = \gamma^{\frac{p^2-1}{3}}.$$

In the first and the last of these cases we get

$$(\beta^{p-1})^{\frac{p+1}{3}} = (\gamma/\beta)^{\frac{p+1}{3}} = 1 \quad \text{or} \quad (\gamma^{p-1})^{\frac{p+1}{3}} = (\beta/\gamma)^{\frac{p+1}{3}} = 1.$$

In either case $p \mid C_{\frac{p+1}{3}}$. In the remaining case we get

$$(\gamma/\beta)^{\frac{p+1}{3}} = (\beta/\gamma)^{\frac{p+1}{3}} \quad \text{or} \quad \beta^{\frac{2(p+1)}{3}} = \gamma^{\frac{2(p+1)}{3}}.$$

If $\beta^{\frac{p+1}{3}} = \gamma^{\frac{p+1}{3}}$, we have $p \mid C_{\frac{p+1}{3}}$. If $\beta^{\frac{p+1}{3}} = -\gamma^{\frac{p+1}{3}}$, then

$$\beta^{p+1} = -\gamma^{p+1} \Rightarrow \beta\gamma = -\gamma\beta,$$

which is impossible. □

There remains the problem of dealing with S primes. If p is an S prime and $p \equiv 1 \pmod 3$ the determination of when $p \mid D_{\frac{p-1}{3}}$ is provided in the following result.

Theorem 5.17. *Let p be an S prime and $p \equiv 1 \pmod 3$. Then $p \mid D_{\frac{p-1}{3}}$ if and only if $p \mid C_{\frac{p-1}{3}}$ and $R^{\frac{p-1}{3}} \equiv 1 \pmod p$.*

Proof. Since p is an S prime, we have zeros α, β, γ of $f(x)$ in $\mathbb{F}_p$ such that

$$\alpha^{\frac{p-1}{3}} = \zeta^i, \quad \beta^{\frac{p-1}{3}} = \zeta^j, \quad \gamma^{\frac{p-1}{3}} = \zeta^k,$$

where $\zeta^2 + \zeta + 1 = 0$. If $p \mid D_{\frac{p-1}{3}}$, then $p \mid C_{\frac{p-1}{3}}$ and two of i, j, k are the same modulo 3. Suppose without loss of generality that $i \equiv j \pmod 3$. If $k \not\equiv i \pmod 3$, then

$$W_{\frac{p-1}{3}} \equiv 0 \not\equiv 6R^{\frac{p-1}{3}} \pmod p,$$

which is impossible. Thus, we must have $i \equiv j \equiv k \pmod 3$ and $R^{\frac{p-1}{3}} \equiv 1 \pmod p$.

If $R^{\frac{p-1}{3}} \equiv 1 \pmod p$ and $p \mid C_{\frac{p-1}{3}}$, then $3 \mid i + j + k$ and two of i, j, k are the same modulo 3. Hence, all three of them must be the same modulo 3 and $p \mid W_{\frac{p-1}{3}} - 6R^{\frac{p-1}{3}}$. □

In the following corollary we will use the sequence A_n as defined in (3.1).

Corollary 5.17.1. *If p is an S prime, $p \equiv 1 \pmod 3$ and $R^{\frac{p-1}{3}} \equiv 1 \pmod p$, then $p \mid D_{\frac{p-1}{3}}$ if and only if $p \nmid A_{\frac{p-1}{3}}$.*

Proof. Since $R^{\frac{p-1}{3}} \equiv 1 \pmod p$, we know that i, j, k in the proof of the theorem are either all the same or all distinct modulo 3. If they are all the same, then $p \nmid A_{\frac{p-1}{3}}$ and $p \mid C_{\frac{p-1}{3}}$, hence $p \mid D_{\frac{p-1}{3}}$ by the above theorem. If they are all distinct, then $p \mid A_{\frac{p-1}{3}}$ and $p \nmid C_{\frac{p-1}{3}}$, so $p \nmid D_{\frac{p-1}{3}}$. □

Chapter 6

Arithmetic Properties of $\{E_n\}$

6.1 Preliminary Results for $\{E_n\}$

While working on the sequences $\{W_n\}$ and $\{C_n\}$, several results developed 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 $(U_n, V_n) \mid 2$ for Lucas functions.

Theorem 6.1. *If* $(Q, R) = 1$, *then* $(D_n, E_n) \mid 6$.

Proof. Suppose 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 $(D_n, R) = (E_n, R)$ and $(D_n, R) \mid 2$ by (5.1), we can only have $p = 2, 3$. If $3^2 \mid (D_n, E_n)$, then $3 \mid R$, which is impossible. If $2^2 \mid (D_n, E_n)$, then $2^2 \mid E_n$, which we have seen by Theorem 4.5 is also impossible. Hence $(D_n, E_n) \mid 6$. □

It is readily apparent that equation (2.12) implies $V_n \mid U_{2n}$. Similarly we have

$$E_n \mid D_{3n}, \tag{6.1}$$

which can be seen as follows. 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

$$W_{3n} - 6R^{3n} \;=\; (W_n - 6R^n)\left(\frac{W_n^2 - \Delta C_n^2}{4}\right) + \Delta W_n C_n^2. \tag{6.2}$$

Recall again from Theorem 4.5 that if $(Q,R)=1$, then $2^\alpha \;||\; (W_n, C_n) \Rightarrow \alpha = 0$ or 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 $E_n \mid D_{3n}$. Clearly we have $C_n \mid C_{3n}$. If $2 \nmid E_n$, then $E_n \mid \tilde{Q}_n \Rightarrow E_n \mid W_{3n} - 6R^{3n}$ by equation (6.2). If $2 \mid E_n$, then $E_n/2$ is odd and $E_n/2 \mid \tilde{Q}_n$. Since $2 \mid W_n$, then $2 \mid W_n - 6R^n \Rightarrow E_n \mid (W_n - 6R^n)\tilde{Q}_n \Rightarrow E_n \mid W_{3n} - 6R^{3n}$ by equation (6.2). Since $E_n \mid C_n$ and $C_n \mid C_{3n}$, we get $E_n \mid C_{3n}$ and $E_n \mid W_{3n} - 6R^{3n} \Rightarrow E_n \mid D_{3n}$.

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

Theorem 6.2. *If $(Q,R)=1$ and $p>3$ is a prime dividing E_n, then $p \equiv 1 \pmod 3$.*

Proof. First note $p \mid W_n \Rightarrow A_n B_n \equiv 3R^n \pmod p$. Also remember $p \nmid R$ as $(W_n, C_n, R) \mid 2$. Since $p \mid (W_n, C_n)$ and $\frac{W_n^2 - \Delta C_n^2}{4} \in \mathbb{Z}$ we have $p \mid \frac{W_n^2 - \Delta C_n^2}{4}$. Replacing W_n^2 by $(A_n B_n - 3R^n)^2$ and ΔC_n^2 by $A_n^2 B_n^2 + 18 A_n B_n R^n - 4B_n^3 - 4A_n^3 R^n - 27R^{2n}$ yields

$$p \mid 3B_n^3 + A_n^4 B_n - 3A_n^2 B_n^2 \Rightarrow p \mid B_n(A_n^4 - 3A_n^2 B_n + 3B_n^2).$$

Notice $p \nmid B_n$; for $p \mid B_n \Rightarrow p \mid R$ and this is not possible by Lemma 4.1. Thus,

$$p \mid A_n^4 - 3A_n^2 B_n + 3B_n^2 \Rightarrow p \mid 4A_n^4 - 12A_n^2 B_n + 12B_n^2 \Rightarrow p \mid (2A_n^2 - 3B_n)^2 + 3B_n^2.$$

But this implies $(2A_n^2 - 3B_n)^2 \equiv -3B_n^2 \pmod p \Rightarrow (\frac{-3B_n^2}{p}) = 1 \Rightarrow (\frac{-3}{p}) = 1$. $\square$

Thus, if p is a prime such that $p > 3$, $p \equiv -1 \pmod 3$ and $p \mid D_{3n}$, we know that $p \nmid E_n$. However, as shown in the next theorem we can say that if $p \mid D_{3n}$ and $p \mid C_n$, then $p \mid D_n$ or $p \mid E_n$.

Theorem 6.3. *Let p be a prime such that $p > 3$. If $p \mid D_{3n}$ and $p \mid C_n$, then $p \mid D_n$ or $p \mid E_n$.*

Proof. From Corollary 3.10.1, we see that

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

Thus, if $p \mid C_n$ and $p \mid D_{3n}$, then $p \mid W_n^2(W_n - 6R^n)$. If $p \nmid E_n$, then $p \nmid W_n$. It follows, then, that $p \mid W_n - 6R^n$ and, therefore, $p \mid D_n$. □

Corollary 6.3.1. *Let p be a prime such that $p > 3$ and $p \equiv -1 \pmod 3$. If $p \mid D_{3n}$, then*

$$p \mid D_n \Leftrightarrow p \mid C_n.$$

Proof. Since $p \equiv -1 \pmod 3$, we cannot have $p \mid E_n$ by Theorem 6.2. Thus, if $p \mid C_n$, then $p \mid D_n$ by Theorem 6.3. □

Theorem 6.4. *Let p be a prime such that $p > 3$ and $p \equiv -1 \pmod 3$. If $p \mid D_{3n}$, then*

$$p \nmid D_n \Leftrightarrow p \mid C_{3n}/C_n.$$

Proof. First we will show ($\Leftarrow$). Assume that $p \mid C_{3n}/C_n$ and $p \mid D_n$. Since $p \mid D_n$, we have $p \mid C_n$. By Corollary 3.10.1, we have

$$4C_{3n}/C_n = \Delta C_n^2 + 3W_n^2;$$

thus, since $p \mid C_n$ and $p \mid C_{3n}/C_n$, we have $p \mid W_n$. Hence $p \mid E_n$ and $p \equiv -1 \pmod 3$, which is a contradiction to Theorem 6.2.

Now suppose that $p \mid D_{3n}$ and $p \nmid D_n$. By Corollary 6.3.1, we cannot have $p \mid C_n$; hence, if $p \mid C_{3n}$, then $p \mid C_{3n}/C_n$. □

We also have a result which tells us when $p \mid D_{3n}$ and $p \nmid C_n$.

Theorem 6.5. *Suppose p is a prime such that $p \nmid 6\Delta$. Then $p \mid D_{3n}$ and $p \nmid C_n$ if and only if*

$$W_n \equiv -3R^n, \;\; \Delta C_n^2 \equiv -27R^{2n} \pmod p.$$

Proof. Suppose $W_n \equiv -3R^n$, $\Delta C_n^2 \equiv -27R^{2n} \pmod p$. Since

$$4C_{3n}/C_n = \Delta C_n^2 + 3W_n^2 \equiv 0 \pmod p,$$

we get $p \mid C_{3n}/C_n$. If $p \mid R$, then $p \mid (C_n, W_n)$, which is impossible because

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

by Lemma 4.6 and $p \neq 2$. Thus, $p \nmid 3R$ and hence $p \nmid C_n$. Also, since

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

we find that $p \mid W_{3n} - 6R^{3n}$ and hence $p \mid D_{3n}$.

Now suppose that $p \mid D_{3n}$ and $p \nmid C_n$. Since $p \mid C_{3n}$, we get

$$p \mid C_n(\Delta C_n^2 + 3W_n^2)$$

and it follows that

$$\Delta C_n^2 \equiv -3W_n^2 \pmod p.$$

Since $p \nmid C_n$ and $p \nmid \Delta$, we cannot have $p \mid W_n$. Also, $p \mid W_{3n} - 6R^{3n}$ implies

$$p \mid 3\Delta C_n^2 W_n + 6\Delta C_n^2 R^n + W_n^2(W_n - 6R^n)$$

and therefore $p \mid 8W_n^2(W_n + 3R^n)$. Thus, we must have

$$W_n \equiv -3R^n, \quad \text{and} \quad \Delta C_n^2 \equiv -27R^{2n} \pmod{p}.$$

□

We next eliminate the possibility that an I prime could divide E_n.

Theorem 6.6. *If p is an I prime, then $p \nmid E_n$.*

Proof. Consider the zeros, α, β, γ, of $f(x)$ in $\mathbb{F}_{p^3}$. We have $\alpha^p = \beta$, $\beta^p = \gamma$, $\gamma^p = \alpha$. If $p \mid C_n$, then without loss of generality $\alpha^n = \beta^n$ in $\mathbb{F}_{p^3}$. So then $\alpha^{pn} = \beta^{pn} \Rightarrow \beta^n = \gamma^n \Rightarrow \alpha^n = \beta^n = \gamma^n$. Hence $W_n = 6\alpha^{3n} = 6R^n$ in $\mathbb{F}_{p^3}$. It follows that $W_n \equiv 6R^n \pmod{p}$. Since $(W_n, C_n, R) \mid 2$ by Lemma 4.6, we must have $p \nmid E_n$.

□

Theorem 6.2 can now be generalized.

Theorem 6.7. *If p is a prime, $p > 3$ and $p \mid E_n$, then $p \equiv 1 \pmod{3^{\nu+1}}$, where $3^\nu \mid\mid n$.*

Proof. Since $(E_n, R) \mid 2$, we must have $p \nmid R$. Suppose $p \mid E_n$. Then we know that p cannot be an I prime by Theorem 6.6 and $p \equiv 1 \pmod 3$ by Theorem 6.2. We also have $p \mid D_{3n}$. If $p \mid D_n$, then $p \mid W_n$ and $p \mid W_n - 6R^n \Rightarrow p \mid 6R^n$, which is a contradiction. Hence $p \nmid D_n$. Let ω be the rank of apparition of p in $\{D_n\}$; we have $\omega(p) \mid 3n$, $\omega(p) \nmid n$, 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 5.6 for the S and Q prime cases. Hence,

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

Since $3 \mid \omega(p)$, we know $\omega(p) \nmid p$. Also, since $3 \mid p-1$, we must have

$$3^{\nu+1} \mid p-1 \Rightarrow p \equiv 1 \pmod{3^{\nu+1}}.$$

□

Lucas showed (Theorem 2.20) 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 $p \neq 2, 3$ such that $p \mid D_{3n}/D_n$.

Theorem 6.8. *If p is a prime, $p > 3$ and $p \mid D_{3n}/D_n$, 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 (5.1), which is not possible. Thus, $p \nmid R$. Also, since $(D_{3n}/D_n, D_n) \mid 27$ by Theorem 5.13, we cannot have $p \mid D_n$. It follows by the same reasoning used in the proof of Theorem 6.7, that

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

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

We next produce some conditions on those primes p such that $p \nmid E_n$ and p is not an I prime.

Theorem 6.9. *If p ($\equiv 1 \pmod 3$) is a Q prime or an S prime, then $p \nmid E_n$ if $3 \nmid \frac{p-1}{3}$ and $R^{\frac{p-1}{3}} \equiv 1 \pmod p$.*

Proof. Let $\mathbb{K}$ be the splitting field of $f(x) \in \mathbb{F}_p[x]$ and let $\alpha(\in \mathbb{F}_p)$, β, γ, be the zeros of $f(x)$ in $\mathbb{K}$. If $p \mid C_n$, then either $\alpha^n = \beta^n$ or $\beta^n = \gamma^n$ or $\alpha^n = \gamma^n$ in $\mathbb{K}$. Without loss of generality assume $\beta^n = \gamma^n$; then $W_n = 2\alpha^{2n}\beta^n + 2\alpha^n\beta^{2n} + 2\beta^{3n} = 2\beta^n(\beta^{2n} + \alpha^n\beta^n + \alpha^{2n})$ in $\mathbb{K}$. Suppose $p \mid E_n$. Since $p \nmid R$ we have $\beta^n \neq 0$; thus, since $p \mid W_n$, there exists $\zeta \in \mathbb{K}$ such that $\zeta^2 + \zeta + 1 = 0$ and $\beta^n = \zeta\alpha^n$. We can then see that

$$R^n = \alpha^n\beta^n\gamma^n = \zeta^2\alpha^{3n} \Rightarrow R^{n(\frac{p-1}{3})} = \zeta^{2(\frac{p-1}{3})}.$$

Thus, if $3 \nmid \frac{p-1}{3}$, we cannot have $R^{\frac{p-1}{3}} = 1$ in $\mathbb{F}_p$. Hence, if $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ and $3 \nmid \frac{p-1}{3}$, then $p \nmid E_n$. □

Notice also that if $3 \mid n$ and $3 \nmid \frac{p-1}{3}$, then $p \nmid E_n$. Further, if $3 \nmid n$, $3 \mid \frac{p-1}{3}$ and $R^{\frac{p-1}{3}} \not\equiv 1 \pmod{p}$, then $p \nmid E_n$.

We will next derive a law of repetition for $\{E_n\}$.

Theorem 6.10. *If $r \mid E_n$ and $(r, 2) = 1$, then*

$$W_{mn} \equiv \begin{cases} mW_nR^{(m-1)n} \pmod{r^2} & \text{if } m \equiv 1 \pmod 3 \\ -mW_nR^{(m-1)n} \pmod{r^2} & \text{if } m \equiv -1 \pmod 3 \\ 6R^{mn} \pmod{r^2} & \text{if } m \equiv 0 \pmod 3 \end{cases}$$

and

$$\frac{C_{mn}}{C_n} \equiv \begin{cases} mR^{(m-1)n} \pmod{r} & \text{if } m \equiv 1, -1 \pmod 3 \\ 0 \pmod{r} & \text{if } m \equiv 0 \pmod 3. \end{cases}$$

Proof. Our assumptions directly imply $r \mid W_n$ and $r^2 \mid \frac{W_n^2 - \Delta C_n^2}{4}$. As before, let $\tilde{P}_n = W_n$ and $\tilde{Q}_n = \frac{W_n^2 - \Delta C_n^2}{4}$. Then it can be shown by induction that $r^{k-1} \mid U_k(\tilde{P}_n, \tilde{Q}_n)$ and $r^k \mid V_k(\tilde{P}_n, \tilde{Q}_n)$.

Now use equations (2.7) and (2.8) as written below

$$2\tilde{Q}_n^{\lambda_2}U_{\lambda_1-\lambda_2} = U_{\lambda_1}V_{\lambda_2} - V_{\lambda_1}U_{\lambda_2} \quad \text{and} \quad 2\tilde{Q}_n^{\lambda_2}V_{\lambda_1-\lambda_2} = V_{\lambda_1}V_{\lambda_2} - \tilde{\Delta}_n U_{\lambda_1}U_{\lambda_2}$$

to see that

$$r^{\lambda_1+\lambda_2-1} \mid \tilde{Q}_n^{\lambda_2}U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) \quad \text{and} \quad r^{\lambda_1+\lambda_2} \mid \tilde{Q}_n^{\lambda_2}V_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n).$$

We now consider W_{mn} and C_{mn}/C_n under the three conditions for $m \pmod 3$. If $\lambda_1 + \lambda_2 \geq 2$, then certainly

$$r \mid \tilde{Q}_n^{\lambda_2}U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) \quad \text{and} \quad r^2 \mid \tilde{Q}_n^{\lambda_2}V_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n).$$

The remaining cases are:

1. if $\lambda_1 = 1$, $\lambda_2 = 0$, then $m \equiv 1 \pmod 3$,
2. if $\lambda_1 = 0$, $\lambda_2 = 1$, then $m \equiv -1 \pmod 3$,
3. if $\lambda_1 = 0$, $\lambda_2 = 0$, then $m \equiv 0 \pmod 3$.

Case 1. $m \equiv 1 \pmod 3$. By use of Theorem 3.14 we have

$$W_{mn} \equiv (-1)^{\lambda_0}\frac{m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!}\tilde{Q}_n^{\lambda_2}V_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) \pmod{r^2}.$$

This can be further simplified using the facts $\lambda_1 = 1$, $\lambda_2 = 0$ and $\lambda_0+\lambda_1+\lambda_2+\lambda_3 = m \Rightarrow \lambda_0+\lambda_3 = m-1 \Rightarrow m-1-\lambda_0 = \lambda_3$. Further, we can see $\lambda_1+2\lambda_2+3\lambda_3 = m \Rightarrow m = 3\lambda_3 - 1 \Rightarrow m \equiv \lambda_3 - 1 \pmod 2$. Since $\lambda_0 = m-1-\lambda_3 \Rightarrow \lambda_0 \equiv m-1-\lambda_3 \pmod 2$ and $m \equiv \lambda_3 - 1 \pmod 2 \Rightarrow 2 \mid \lambda_0$. So

$$W_{mn} \equiv mW_nR^{(m-1)n} \pmod{r^2}.$$

Similarly,

$$\frac{C_{mn}}{C_n} \equiv mR^{(m-1)n} \pmod{r}.$$

Case 2. $m \equiv -1 \pmod 3$.

Now since $\lambda_1 = 0$, $\lambda_2 = 1$ and $\lambda_0+\lambda_1+\lambda_2+\lambda_3 = m \Rightarrow \lambda_0+\lambda_3 = m-1 \Rightarrow m-1-\lambda_0 = \lambda_3$. Also $\lambda_0 = m-1-\lambda_3 \Rightarrow \lambda_0 \equiv m-1-\lambda_3 \pmod 2$ but $\lambda_1 + 2\lambda_2 + 3\lambda_3 = m \Rightarrow 2 + 3\lambda_3 = m \Rightarrow \lambda_3 \equiv m \pmod 2 \Rightarrow 2 \nmid \lambda_0$. So

$$\begin{aligned} W_{mn} &\equiv (-1)mR^{(m-1)n}\tilde{Q}_n V_{-1}(\tilde{P}_n, \tilde{Q}_n) \pmod{r^2} \\ &\equiv -mR^{(m-1)n}V_1(\tilde{P}_n, \tilde{Q}_n) \pmod{r^2} \\ &\equiv -mR^{(m-1)n}W_n \pmod{r^2}. \end{aligned}$$

Similarly,

$$\frac{C_{mn}}{C_n} \equiv mR^{(m-1)n} \pmod{r}.$$

Case 3. $m \equiv 0 \pmod 3$.

Here $\lambda_1 = \lambda_2 = 0 \Rightarrow \lambda_0+\lambda_3 = m$ and $3\lambda_3 = m$. So $\lambda_3 \equiv m \pmod 2$ and $\lambda_0 \equiv m-\lambda_3 \pmod 2$ yields $\lambda_0 \equiv 0 \pmod 2$. Hence

$$\begin{aligned} W_{mn} &\equiv (-1)^{\lambda_0}\frac{m(m-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!}R^{(\lambda_0+\lambda_3)n}\tilde{Q}_n^{\lambda_2}V_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n) \pmod{r^2} \\ &\equiv (-1)^0\frac{3\lambda_3(\lambda_3-1)!}{\lambda_3!}R^{(m)n}\tilde{Q}_n^0 V_0(\tilde{P}_n, \tilde{Q}_n) \pmod{r^2} \\ &\equiv 6R^{mn} \pmod{r^2}. \end{aligned}$$

Similarly, since $U_0 = 0$

$$\frac{C_{mn}}{C_n} \equiv 0 \pmod{r}.$$

□

Corollary 6.10.1. *If p is any prime such that $p > 3$ and $p \mid E_n$, then $p \nmid E_{mn}$ when $3 \mid m$.*

Corollary 6.10.2. *If p is any odd prime and $p^\mu \mid\mid E_n$ $(\mu \geq 1)$, then $p^\mu \mid\mid E_{mn}$ when $p \nmid m$ and $3 \nmid m$.*

The case of $p = 3$ is contained in the next two corollaries.

Corollary 6.10.3. *If $3^\mu \mid\mid E_n$, then $3 \mid\mid E_{mn}$ when $3 \mid m$.*

Corollary 6.10.4. *If $3^\mu \mid\mid E_n$, then $3^\mu \mid\mid E_{mn}$ when $3 \nmid m$.*

Of course, when $p = 2$, we know that $2^\mu \mid\mid E_n \Rightarrow \mu = 0$ or 1. From this, Corollary 3.10.1 and Theorem 4.5, we see that if $2 \mid\mid E_n$, then $2 \mid\mid E_{2n}$. Also, since $4 \mid W_n^2 - \Delta C_n^2$, we see that $2 \mid E_n \Leftrightarrow 2 \mid C_n$.

Theorem 6.11. *If p is a prime such that $p > 3$ and $p^\mu \mid\mid E_n$, then $p^{\mu+1} \mid\mid E_{pn}$ for $\mu \geq 1$.*

Proof. We note that $p \mid \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!}$ 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 the previous theorem, $(p^\mu)^p \mid V_p(\tilde{P}_n, \tilde{Q}_n)$ 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 $\lambda_1 + \lambda_2 \geq 2 \Rightarrow p^{2\mu+1} \mid \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} \tilde{Q}_n^{\lambda_2} V_{\lambda_1-\lambda_2}$.

Similarly, $p^{\mu} \mid \tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}(\tilde{P}_n, \tilde{Q}_n)$ for $\lambda_1 + \lambda_2 \geq 2 \Rightarrow p^{\mu+1} \mid \frac{p(p-\lambda_0-1)!}{\lambda_1!\lambda_2!\lambda_3!} \tilde{Q}_n^{\lambda_2} U_{\lambda_1-\lambda_2}$. Thus we need only concern ourselves with the case $\lambda_1 + \lambda_2 = 1$, which yields

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

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 $\tilde{\Delta}_n = \Delta C_n^2 \Rightarrow p \nmid \tilde{\Delta}_n \Rightarrow U_p(\tilde{P}_n, \tilde{Q}_n) \not\equiv 0 \pmod{p}$. But $\frac{C_{pn}}{C_n} \equiv U_p(\tilde{P}_n, \tilde{Q}_n) \pmod{p}$, so $p \nmid C_{pn}$. Also, since if $p \mid C_n$, then $p \mid W_n \Leftrightarrow p \mid W_{pn}$, we see that $p \nmid E_{pn}$ when $p \nmid W_n$.

6.2 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 Chapter 2 that were, until now, missing. We must first deal with the case of $p = 2$. Since $2 \mid E_n \Leftrightarrow 2 \mid C_n$, from our results in Section 4.1, there always exists some minimal ρ 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 3.10.1 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 $E_n \mid E_{2n}$.

Lemma 6.12. *If $r \mid E_m$, $r \mid E_n$ and $(r, 2) = 1$, then $r \mid E_{3n+m}$.*

Proof. We interchange m and n in Corollary 3.10.2 to obtain

$$\begin{aligned} 2W_{3n+m} &= W_nW_{2n+m} + \Delta C_nC_{2n+m} - R^nW_nW_{n+m} + R^n\Delta C_nC_{n+m} + 2R^{3n}W_m \\ 2C_{3n+m} &= W_nC_{2n+m} + C_nW_{2n+m} - R^nW_nC_{n+m} + R^nC_nW_{n+m} - 2R^{3n}C_m. \end{aligned}$$

The proof follows immediately. □

We will say $r \mid E_n$ when $n < 0$ if $r \mid E_{|n|}$.

Lemma 6.13. *If $r \mid E_m$ and $r \mid E_n$, then $r \mid E_{3n+m}$.*

Proof. Note that if $2 \mid r$, then $2 \nmid \frac{r}{2}$ as $4 \nmid (W_n, C_n)$ as seen in Theorem 4.5. By the previous lemma we have $\frac{r}{2} \mid E_{3n+m}$. Now since $\frac{W_n^2 - \Delta C_n^2}{4} \in \mathbb{Z}$ we have $2 \mid E_n \Leftrightarrow 2 \mid C_n$. So we need only show $2 \mid C_m$ and $2 \mid C_n$ implies $2 \mid C_{3n+m}$. There exists some minimal ρ such that $2 \mid C_\rho$. Moreover, if $2 \mid C_n$, then $\rho \mid n$. Thus $n = k_1\rho$ and $m = k_2\rho$. Hence $2 \mid C_{(3k_1+k_2)\rho} \Rightarrow 2 \mid C_{3n+m}$, which concludes the proof. □

Theorem 6.14. *If $r \mid E_m$ and $r \mid E_n$, then $r \mid E_{3kn+m}$ for $k \geq 1$.*

Proof. Proceed by induction using the previous lemma. Clearly it is true for $k = 1$. Assume this is true for $r \mid E_{3kn+m}$. We also have $r \mid E_n$. So by the previous lemma, if we replace m by $3kn + m$, we have $r \mid E_{3n+3kn+m} \Rightarrow r \mid E_{3(k+1)n+m}$. □

Corollary 6.14.1. *If $3 \nmid m$, then $E_n \mid E_{mn}$.*

Proof. Since $3 \nmid m$, we must have $m = 3k + 1$ or $m = 3k + 2$. Since $E_n \mid E_{2n}$, we have $E_n \mid E_{3kn+n}$ and $E_n \mid E_{3kn+2n}$. Hence $E_n \mid E_{mn}$, when $3 \nmid m$. □

We are now able to provide an analogue to Theorem 2.14.

Theorem 6.15. *Suppose $r \mid E_n$, $(n > 0)$, then there must be a least positive $\rho = \rho(r)$ such that $r \mid E_\rho$. Further, $\rho \mid n$.*

Proof. Clearly, since $r \mid E_n$, such a value for ρ must exist. Let $3^\mu \mid\mid (n, \rho)$.

Case 1: $3^\mu \mid\mid n$

In this case put $d_1 = (3\rho, n) \Rightarrow 3^\mu \mid\mid d_1$. Since

$$d_1 = 3\rho x + ny \quad \text{where} \quad x, y \in \mathbb{Z}$$

we get

$$\frac{d_1}{3^\mu} = \frac{3\rho x}{3^\mu} + \frac{ny}{3^\mu}.$$

Thus $3 \nmid y$ as $3 \nmid \frac{d_1}{3^\mu}$ and $3 \mid \frac{3\rho}{3^\mu}$.

Let $3^k \mid\mid x$. Since $r \mid E_{\frac{x\rho}{3^k}}$ and $r \mid E_{yn}$ by Corollary 6.10.2 we see from Theorem 6.14 that

$$r \mid E_{3\rho x + yn} \Rightarrow r \mid E_{d_1}.$$

We know $d_1 \geq \rho$ by minimality of ρ. But $d_1 \mid 3\rho \Rightarrow \frac{d_1}{3^\mu} \mid \frac{3\rho}{3^\mu}$. Since $3 \nmid \frac{d_1}{3^\mu}$ we have $d_1 \mid \rho \Rightarrow \rho = d_1$. Since $d_1 \mid n$, we have $\rho \mid n$.

Case 2: $3^\mu \mid\mid \rho$

In this case put $d_2 = (\rho, 3n) \Rightarrow 3^\mu \mid\mid d_2$. Hence

$$d_2 = 3nz + \rho w \quad \text{where} \quad z, w \in \mathbb{Z}.$$

Thus

$$\frac{d_2}{3^\mu} = \frac{3z}{3^\mu} + \frac{\rho w}{3^\mu} \Rightarrow 3 \nmid w.$$

Reasoning as before with $3^k \mid\mid z$, we get

$$r \mid E_{3nz + \rho w} \Rightarrow r \mid E_{d_2} \Rightarrow d_2 \geq \rho.$$

Since $d_2 \mid \rho \Rightarrow d_2 = \rho$. Also $\rho \mid 3n \Rightarrow \frac{\rho}{3^\mu} \mid \frac{n}{3^\mu} \Rightarrow \rho \mid n$.

□

6.3 Further Observations on the Law of Apparition for $\{E_n\}$

We next examine the problem of determining some m such that $p \mid E_m$ when p is a prime and $(p, 6R\Delta) = 1$. Although it may not seem obvious, the next theorem is part of our extension of Euler's criterion, this will become more apparent later in the chapter as several theorems concerning $\{E_n\}$ and $\{D_n\}$ lend themselves to the generalization of this result. We note that if p is a Q prime, then $W_{p^2-1} \equiv 6 \pmod{p}$ by (4.15). Hence $p \nmid E_{p^2-1}$. However, it is possible that $p \mid E_{\frac{p^2-1}{3}}$. We also recall from Theorem 6.2 that if $p \mid E_n$ for any n, then $p \equiv 1 \pmod{3}$.

Theorem 6.16. *If p ($\equiv 1 \pmod 3$) is a Q prime, then*

$$p \mid E_{\frac{p^2-1}{3}} \Leftrightarrow R^{\frac{p-1}{3}} \not\equiv 1 \pmod{p}.$$

Proof. We have α, β, γ as the zeros of $f(x)$ in $\mathbb{F}_{p^2}$ such that

$$\alpha^p = \alpha, \quad \beta^p = \gamma \quad \text{and} \quad \gamma^p = \beta.$$

Hence,

$$\alpha^{p-1} = 1, \quad \alpha^{p+1} = \alpha^2, \quad \beta^{p+1} = \beta\gamma \quad \text{and} \quad \gamma^{p+1} = \beta\gamma.$$

Now $\beta\gamma = R/\alpha$ and

$$\begin{aligned} \beta^{\frac{p^2-1}{3}} = \gamma^{\frac{p^2-1}{3}} &= (\beta\gamma)^{\frac{p-1}{3}} = \left(\frac{R}{\alpha}\right)^{\frac{p-1}{3}} = \frac{R^{\frac{p-1}{3}}}{\alpha^{\frac{p-1}{3}}} \cdot \frac{\alpha^{\frac{2(p-1)}{3}}}{\alpha^{\frac{2(p-1)}{3}}} = R^{\frac{p-1}{3}} \alpha^{\frac{2(p-1)}{3}} \\ &= R^{\frac{p-1}{3}} (\alpha^2)^{\frac{p-1}{3}} = R^{\frac{p-1}{3}} (\alpha^{p+1})^{\frac{p-1}{3}} = R^{\frac{p-1}{3}} \alpha^{\frac{p^2-1}{3}}. \end{aligned}$$

It then follows that $p \mid C_{\frac{p^2-1}{3}}$ and

$$W_{\frac{p^2-1}{3}} \equiv 2\alpha^{p^2-1}(1 + R^{\frac{p-1}{3}} + R^{\frac{2(p-1)}{3}}) \equiv 2(1 + R^{\frac{p-1}{3}} + R^{\frac{2(p-1)}{3}}) \pmod{p}.$$

We can then see

$$R^{\frac{p-1}{3}} \not\equiv 1 \pmod{p} \Leftrightarrow 1 + R^{\frac{p-1}{3}} + R^{2\frac{p-1}{3}} \equiv 0 \pmod{p} \Leftrightarrow p \mid W_{\frac{p^2-1}{3}}.$$

□

We next consider the possibility that $p \mid E_{p+1}$ when p is a Q prime. In this case $p \neq 3$ and $p \equiv 1 \pmod 3$ by Theorem 6.2. We already know that $p \mid C_{p+1}$ by Corollary 4.24.1. Let α, β, γ be the zeros of $f(x)$ in $\mathbb{F}_{p^2}$, then $\alpha^p = \alpha$, $\beta^p = \gamma$, $\gamma^p = \beta$. Then we have $\alpha^{p+1} = \alpha^2$, $\beta^{p+1} = \gamma\beta$, $\gamma^{p+1} = \gamma\beta$. So

$$\begin{aligned} W_{p+1} &= (\alpha^{p+1}\beta^{2p+2} + \beta^{p+1}\gamma^{2p+2} + \gamma^{p+1}\alpha^{2p+2}) + (\alpha^{2p+2}\beta^{p+1} + \beta^{2p+2}\gamma^{p+1} + \gamma^{2p+2}\alpha^{p+1}) \\ &= (\alpha^2\beta^2\gamma^2 + \beta^3\gamma^3 + \alpha^4\beta\gamma) + (\alpha^4\beta\gamma + \beta^3\gamma^3 + \beta^2\gamma^2\alpha^2) \\ &= 2(\alpha^4\beta\gamma + \alpha^2\beta^2\gamma^2 + \beta^3\gamma^3). \end{aligned}$$

Hence, we can see that

$$W_{p+1} \equiv 0 \pmod{p} \Leftrightarrow \alpha^4\beta\gamma + (\alpha\beta\gamma)^2 + (\beta\gamma)^3 = 0 \Leftrightarrow \ \alpha^2 = \zeta\beta\gamma \text{ or } \alpha^2 = \zeta^2\beta\gamma$$

where $\zeta^2 + \zeta + 1 = 0$. Note $p \equiv 1 \pmod 3 \Rightarrow \zeta \in \mathbb{F}_p$.

Now consider

$$M_1 = (\alpha^2 - \zeta\beta\gamma)(\beta^2 - \zeta\alpha\gamma)(\gamma^2 - \zeta\alpha\beta)$$

$$M_2 = (\alpha^2 - \zeta^2\beta\gamma)(\beta^2 - \zeta^2\alpha\gamma)(\gamma^2 - \zeta^2\alpha\beta).$$

Clearly then $M_1M_2 = 0$, when $W_{p+1} = 0$, as $W_{p+1} = 0$ if and only if $\alpha^2 = \zeta\beta\gamma$ or $\alpha^2 = \zeta^2\beta\gamma$. Also if $M_1M_2 = 0$, then $W_{p+1} = 0$. This is obvious for the cases

$\alpha^2-\zeta\beta\gamma = 0$ and $\alpha^2-\zeta^2\beta\gamma = 0$, so suppose $\beta^2-\zeta\alpha\beta = 0 \Rightarrow \beta^{2(p+1)} = \zeta^{p+1}(\alpha\beta)^{p+1} \Rightarrow (\beta\gamma)^2 = \zeta^{p+1}\alpha^2\beta\gamma \Rightarrow \beta\gamma = \zeta^{p+1}\alpha^2 \Rightarrow \alpha^2 = \zeta^{-(p+1)}\beta\gamma \Rightarrow \alpha^2 = \zeta\beta\gamma$. Similarly for any of the other 3 factors of M_1M_2.

Now

$$\begin{aligned} M_1 &= (\alpha^2-\zeta\beta\gamma)(\beta^2-\zeta\alpha\gamma)(\gamma^2-\zeta\alpha\beta) \\ &= \alpha^2\beta^2\gamma^2 - \zeta\alpha^3\gamma^3 - \zeta\beta^3\gamma^3 - \zeta\alpha^3\beta^3 + \zeta^2\alpha\beta\gamma^4 + \zeta^2\alpha^4\beta\gamma + \zeta^2\alpha\beta^4\gamma - \zeta^3\zeta^2\alpha^2\beta^2\gamma^2 \\ &= \zeta^2(\alpha\beta\gamma)(\alpha^3+\beta^3+\gamma^3) - \zeta((\alpha\beta)^3+(\beta\gamma)^3+(\gamma\alpha)^3) \\ &= \zeta^2RA_3 - \zeta B_3. \end{aligned}$$

Also $M_2 = \zeta RA_3 - \zeta^2B_3$. So

$$\begin{aligned} M_1M_2 &= (\zeta^2RA_3-\zeta B_3)(\zeta RA_3-\zeta^2B_3) \\ &= \zeta^3R^2A_3^2 - \zeta^2RA_3B_3 - \zeta^4RA_3B_3 + \zeta^3B_3^2 \\ &= R^2A_3^2 - \zeta^2RA_3B_3 - \zeta RA_3B_3 + B_3^2 \\ &= (RA_3)^2 + RA_3B_3 + B_3^2. \end{aligned}$$

Hence, $p \mid W_{p+1} \Leftrightarrow p \mid (RA_3)^2 + RA_3B_3 + B_3^2$. Thus, if p is a Q prime, then $p \mid E_{p+1} \Leftrightarrow p \mid M_1M_2$.

Remember $A_3 = P^3-3PQ+3R$ and $B_3 = Q^3-3PQR+3R^2$. Since only a finite number of primes can divide M_1M_2, there can only be a finite number of Q primes p such that $p \mid W_{p+1}$, which means that there can only be a finite number of primes p such that $p \mid W_r$, where r is the rank of apparition of p for $\{C_n\}$. For if $p \mid W_r$, then $p \mid E_{p+1}$ because $r \mid p+1$ and $3 \nmid p+1$, by Corollary 6.10.2.

We now produce a result similar to Theorem 6.16 for S primes. Let α, β, γ be the zeros of $f(x)$ in $\mathbb{K}$, where $p \equiv 1 \pmod 3$ is an S prime. Suppose that there exists

$\rho = \rho(p)$ such that $p \mid E_\rho$, $\rho > 1$ and ρ is minimal. Then $\rho = kr_1$ where r_1 is some rank of apparition of p in $\{C_n\}$. Suppose further that $r_1 \mid 3n$ and

$$(\alpha/\beta)^n = \zeta^i, \quad (\beta/\gamma)^n = \zeta^j, \quad \text{where} \quad \zeta^2 + \zeta + 1 = 0 \quad \text{in } \mathbb{K}.$$

This is certainly the case when $n = (p-1)/3$. Note that $\alpha^n = \zeta^i\beta^n$ and $\beta^n = \zeta^j\gamma^n \Rightarrow \alpha^n = \zeta^{i+j}\gamma^n$. Also since $(\zeta - 1)(\zeta^2 + \zeta + 1) = 0 \Rightarrow \zeta^3 = 1$, we have $\alpha^{3n} = \beta^{3n} = \gamma^{3n}$. Thus $W_{3n} = 6R^{3n} \pmod p$.

We distinguish 3 cases:

Case 1: $3 \nmid ij(i+j)$

Since $\alpha^n = \zeta^i\beta^n$, $\beta^n = \zeta^j\gamma^n$, $\alpha^n = \zeta^{i+j}\gamma^n$ and $3 \nmid ij(i+j)$ we see that α^n, β^n, γ^n are pairwise distinct. Thus $p \nmid C_n \Rightarrow r_1 \nmid n \Rightarrow 3 \nmid \frac{3n}{r_1}$. Since $p \mid C_\rho$ and $p \mid W_\rho$, we must have $p \mid W_{\frac{3n}{r_1}\rho}$ by Corollary 6.10.2 and hence $p \mid W_{3nk}$. Since $W_{3nk} \equiv 6R^{3nk} \pmod p$, this is impossible.

Case 2: 3 divides only one of i, j, $(i+j)$

In this case $p \mid C_n$, since without loss of generality $\alpha^n = \beta^n$, so $3 \mid i$ and $3 \nmid j$. Using $\alpha^n = \beta^n = \zeta^j\gamma^n$,

$$\begin{aligned} W_n &= (\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n) + (\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}) \\ &= (\zeta^{2j}\gamma^{2n}\zeta^j\gamma^n + \zeta^{2j}\gamma^{2n}\gamma^n + \gamma^{2n}\zeta^j\gamma^n) + (\zeta^j\gamma^n\zeta^{2j}\gamma^{2n} + \zeta^j\gamma^n\gamma^{2n} + \gamma^n\zeta^{2j}\gamma^{2n}) \\ &= 2\gamma^{3n}(1 + \zeta^j + \zeta^{2j}) \\ &= 0 \quad \text{since} \quad 3 \nmid j \Rightarrow 1 + \zeta^j + \zeta^{2j} = 0. \end{aligned}$$

So $p \mid E_n$. Thus ρ exists and $\rho \mid n$.

Case 3: 3 divides 2 of i, j, $(i+j)$

Since 3 divides two of i, j, $(i+j)$, it divides all of them. Hence $\alpha^n = \beta^n = \gamma^n \Rightarrow p \mid C_n$ and $W_n = 6R^n \pmod{p}$.

Subcase 1: $r_1 \nmid n$.

Since $r_1 \mid 3n$, we know that $3 \nmid \frac{3n}{r_1} \Rightarrow p \mid W_{3nk}$, which is impossible.

Subcase 2: $r_1 \mid n$

If $3 \nmid n$, then $3 \nmid \frac{n}{r_1}$ and by Corollary 6.10.2 we have $p \mid W_{\frac{n}{r_1}\rho} \Rightarrow p \mid W_{kn}$. This is a contradiction, as $W_{kn} \equiv 6R^{kn} \pmod{p}$. Thus, if ρ exists, then $\rho = kr_1$, where $r_1 \mid n$ and $3 \mid n$ and $(\alpha/\beta)^{n/3} = \zeta^i$, $(\beta/\gamma)^{n/3} = \zeta^j$. By repeating the above argument we see that if ρ exists, then $\rho \mid n/3$.

The fact that whenever ρ exists, $\rho \mid n$ implies in the case that $n = (p-1)/3$, that $(\alpha/\beta)^{(p-1)/3} = \zeta^i$ and $(\beta/\gamma)^{(p-1)/3} = \zeta^j$ and therefore $\rho \mid \frac{p-1}{3}$. Also, $R^{\frac{p-1}{3}} = (\alpha\beta\gamma)^{\frac{p-1}{3}} = \zeta^{i+2j}$, and $3 \mid ij(i^2 - j^2)$. So if $3 \nmid ij(i+j)$, then $3 \mid (i-j)$. If 3 divides only one of i, j, $i+j$, then $3 \nmid i-j$. But if 3 divides all of i, j, $i+j$, then $3 \mid i-j$. Thus ρ exists and $\rho \mid \frac{p-1}{3}$ if $R^{\frac{p-1}{3}} \not\equiv 1 \pmod{p}$. When $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ and $3 \nmid \frac{p-1}{3}$, ρ does not exist. If $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ and $3 \mid \frac{p-1}{3}$, then, if ρ exists, $\rho \mid \frac{p-1}{9}$. We have proved the following theorem.

Theorem 6.17. *If p is an S prime and $p \equiv 1 \pmod{3}$, then*

$$p \mid E_{\frac{p-1}{3}} \Leftrightarrow R^{\frac{p-1}{3}} \not\equiv 1 \pmod{p}.$$

Also, if $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ and $p \not\equiv 1 \pmod{9}$, then $\rho(p)$ cannot exist. If $R^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ and $p \equiv 1 \pmod{9}$, then $\rho \mid \frac{p-1}{9}$ if ρ exists.

We also have the following result.

Theorem 6.18. *If p is an S prime and $p \equiv 1 \pmod 3$, then*

$$p \mid E_{\frac{p^2-1}{3}} \Leftrightarrow p \mid E_{\frac{p-1}{3}}.$$

Proof. Clearly, since $3 \nmid p+1$, $p \mid E_{\frac{p^2-1}{3}}$ when $p \mid E_{\frac{p-1}{3}}$. Next suppose that $p \mid E_{\frac{p^2-1}{3}}$. If α, β, γ are defined as above, we must have

$$\alpha^{\frac{p^2-1}{3}} = \beta^{\frac{p^2-1}{3}} \Rightarrow (\alpha^{p+1})^{\frac{p-1}{3}} = (\beta^{p+1})^{\frac{p-1}{3}} \Rightarrow (\alpha^2)^{\frac{p-1}{3}} = (\beta^2)^{\frac{p-1}{3}}.$$

So, we then have

$$(\alpha^{\frac{p-1}{3}})^2 = (\beta^{\frac{p-1}{3}})^2 \Rightarrow \alpha^{\frac{p-1}{3}} = \pm\beta^{\frac{p-1}{3}}.$$

If $\alpha^{\frac{p-1}{3}} = \beta^{\frac{p-1}{3}}$, then $p \mid C_{\frac{p-1}{3}}$. If $\alpha^{\frac{p-1}{3}} = -\beta^{\frac{p-1}{3}}$, then

$$\alpha^{p-1} = -\beta^{p-1} \Rightarrow 1 = -1,$$

which is impossible. Also, since $p \mid W_{\frac{p^2-1}{3}}$, we get

$$2\alpha^{\frac{p^2-1}{3}}(\alpha^{\frac{2(p^2-1)}{3}} + \gamma^{\frac{p^2-1}{3}}\alpha^{\frac{p^2-1}{3}} + \gamma^{\frac{2(p^2-1)}{3}}) \equiv 0 \pmod p.$$

Since, $p \nmid 2R$, this means that

$$\alpha^{\frac{p^2-1}{3}} = \zeta\gamma^{\frac{p^2-1}{3}}$$

for some ζ such that $\zeta^2 + \zeta + 1 = 0$. It follows that

$$\alpha^{\frac{2(p-1)}{3}} = \zeta\gamma^{\frac{2(p-1)}{3}}.$$

Since $\alpha^{p-1} = \gamma^{p-1} = 1$, we find by squaring that

$$\alpha^{\frac{p-1}{3}} = \zeta^2\gamma^{\frac{p-1}{3}}.$$

Since $p \mid C_{\frac{p-1}{3}}$, we get $p \mid E_{\frac{p-1}{3}}$. □

By similar techniques we can also establish the next result.

Theorem 6.19. *If p is an S prime and $p \equiv 1 \pmod 3$, then*

$$p \mid D_{\frac{p^2-1}{3}} \Leftrightarrow p \mid D_{\frac{p-1}{3}}.$$

Let $\nu_p(x)$ denote that value of ν such that $p^\nu \mid\mid x$, where $x \in \mathbb{Z}^{>0}$ and p is a prime.

Theorem 6.20. *Let p be an S prime and suppose that $\rho = \rho(p)$ exists. In this case $\rho = kr_1$, where r_1 is a rank of apparition of p in $\{C_n\}$. If r_2 is any other rank of apparition of p in $\{C_n\}$, then $\nu_3(r_2) > \nu_3(r_1)$.*

Proof. Since $p \mid E_\rho$, we must have $(\alpha/\beta)^\rho = \zeta^i$, $(\beta/\gamma)^\rho = \zeta^j$ in $\mathbb{F}_p$, where $\zeta^2+\zeta+1 = 0$. Here 3 divides only one of i, j, $i+j$. Without loss of generality suppose $3 \mid i$, then $\beta^\rho = \zeta^j\gamma^\rho$, $\alpha^\rho = \zeta^j\gamma^\rho$ and $3 \nmid j$.

If r_2 is another rank of apparition of p, then it is either the order of β/γ or α/γ in $\mathbb{F}_p$. So $r_2 \mid 3\rho$ and $r_2 \nmid \rho$. Thus if $k = \nu_3(\rho)$ then $\nu_3(r_2) = k+1$. Since $r_1 \mid \rho$, we must have $\nu_3(r_1) \leq \nu_3(\rho) = k < \nu_3(r_2)$. □

To proceed any further we will need the following results for Lucas sequences. Because they seem to be difficult to locate in the literature, proofs are provided here.

Theorem 6.21. *Let V_n, U_n be the Lucas functions $V_n(P,Q)$, $U_n(P,Q)$ and let p be a prime such that $p > 3$ and $(\frac{Q}{p}) = 1$. Let ω be the rank of apparition of p in $\{U_n\}$. Let $S^2 \equiv Q \pmod p$. Then there exists a minimal λ such that*

$$V_\lambda(P,Q) \equiv -S^\lambda \pmod p$$

if and only if $3 \mid \omega$. Furthermore, $\lambda = \omega/3$ or $2\omega/3$.

Proof. ($\Rightarrow$) Suppose λ exists. Then $V_\lambda^2 \equiv Q^\lambda \pmod{p}$ and using $U_{3n} = U_n(V_n^2 - Q^n)$ we see $p \mid U_{3\lambda}$. Also $p \nmid U_\lambda$, for if $p \mid U_\lambda$, then $V_\lambda^2 \equiv 4Q^\lambda \pmod{p}$, as $V_n^2 - \Delta U_n^2 = 4Q^n$, which is not possible. Thus $\omega \mid 3\lambda$ and $\omega \nmid \lambda$, so $3 \mid \omega$.

Put $\mu = \omega/3$. Then $\mu \mid \lambda$. Again, use $U_{3\mu} = U_\mu(V_\mu^2 - Q^\mu)$, knowing $U_{3\mu} \equiv 0 \pmod{p}$ and $U_\mu \not\equiv 0 \pmod{p}$, so $V_\mu^2 \equiv Q^\mu \pmod{p}$. Hence

$$V_\mu(P, Q) \equiv \pm S^\mu \pmod{p}.$$

If $V_\mu \equiv -S^\mu \pmod{p}$, then $\lambda = \mu$ by minimality of λ.

If $V_\mu \equiv S^\mu \pmod{p}$, then $V_{2\mu} \equiv -S^{2\mu} \pmod{p}$, as

$$\begin{aligned} V_{2\mu} &= V_\mu^2 - 2Q^\mu \\ &\equiv Q^\mu - 2Q^\mu \\ &\equiv -S^{2\mu} \pmod{p}. \end{aligned}$$

Thus $\lambda = 2\mu$ by the minimality of λ.

($\Leftarrow$) If $3 \mid \omega$, we must have

$$V_\mu \equiv \pm S^\mu \pmod{p}$$

where $\mu = \omega/3$ as before. Thus $V_\mu \equiv -S^\mu \pmod{p}$ or $V_\mu \equiv S^\mu \pmod{p}$. Thus, there exists a minimal λ such that $V_\lambda(P, Q) \equiv -S^\lambda \pmod{p}$ holds, and we have already seen that $\lambda = \mu$ or $\lambda = 2\mu$. □

One may also notice that if $(\frac{\Delta}{p}) = 1$, where $\Delta = P^2 - 4Q$ and $p \equiv 1 \pmod{3}$, then $p \mid U_{p-1} \Rightarrow \omega \mid p - 1$. Let $3^\mu \mid\mid p - 1$. If $3 \mid \omega$, then $\omega \nmid \frac{p-1}{3^\mu}$. Also if $\omega \nmid \frac{p-1}{3^\mu}$, then $3 \mid \omega$. Thus λ exists if and only if $p \nmid U_{\frac{p-1}{3^\mu}}$.

Theorem 6.22. *If ω is the rank of apparition of p in $\{U_n\}$ and $6 \mid \omega$, then $V_{\frac{\omega}{3}} \equiv Q^{\frac{\omega}{3}} \pmod{p}$.*

Proof. Put $\omega = 6k$. We have $U_{6k} \equiv 0 \pmod{p}$ and using $U_{2n} = U_n V_n$ we get $U_{2(3k)} = U_{3k}V_{3k} \equiv 0 \pmod{p}$. So $V_{3k} \equiv 0 \pmod{p}$ as $U_{3k} \not\equiv 0 \pmod{p}$. Moreover, $V_{\frac{\omega}{2}} \equiv 0 \pmod{p}$ because $p \nmid U_{\frac{\omega}{2}}$. Now, since $V_{2n} = V_n^2 - 2Q^n$ if we set $n = \frac{\omega}{2} \Rightarrow V_\omega = V_{\frac{\omega}{2}}^2 - 2Q^{\frac{\omega}{2}}$. So $V_\omega \equiv -2Q^{\frac{\omega}{2}} \pmod{p}$.

We also know that $V_{3n} = V_n^3 - 3Q^n V_n$; by setting $n = \frac{\omega}{3}$, we get $V_\omega = V_{\frac{\omega}{3}}^3 - 3Q^{\frac{\omega}{3}} V_{\frac{\omega}{3}}$. So

$$\begin{aligned} -2Q^{\frac{\omega}{2}} &\equiv V_{\frac{\omega}{3}}^3 - 3Q^{\frac{\omega}{3}} V_{\frac{\omega}{3}} \pmod{p} \\ \frac{-2Q^{\frac{\omega}{2}}}{Q^{\frac{\omega}{2}}} &\equiv \frac{V_{\frac{\omega}{3}}^3}{Q^{\frac{\omega}{2}}} - \frac{3Q^{\frac{\omega}{3}} V_{\frac{\omega}{3}}}{Q^{\frac{\omega}{2}}} \pmod{p} \\ -2 &\equiv \left(\frac{V_{\frac{\omega}{3}}}{Q^{\frac{\omega}{6}}}\right)^3 - 3\left(\frac{V_{\frac{\omega}{3}}}{Q^{\frac{\omega}{6}}}\right) \pmod{p}. \end{aligned}$$

On putting $T = \frac{V_{\frac{\omega}{3}}}{Q^{\frac{\omega}{6}}}$, we get $T^3 - 3T + 2 \equiv 0 \pmod{p}$ or $(T-1)^2(T+2) \equiv 0 \pmod{p}$.

If $T + 2 \equiv 0 \Rightarrow \frac{V_{\frac{\omega}{3}}}{Q^{\frac{\omega}{6}}} \equiv -2 \Rightarrow V_{\frac{\omega}{3}} \equiv -2Q^{\frac{\omega}{6}} \Rightarrow V_{\frac{\omega}{3}}^2 \equiv 4Q^{2\frac{\omega}{6}} \pmod{p}$. Using $V_n^2 - \Delta U_n^2 = 4Q^n$ with $n = \frac{\omega}{3} \Rightarrow V_{\frac{\omega}{3}}^2 - \Delta U_{\frac{\omega}{3}}^2 = 4Q^{\frac{\omega}{3}} \Rightarrow U_{\frac{\omega}{3}} \equiv 0 \pmod{p}$, which is a contradiction. So $T \equiv 1 \pmod{p} \Rightarrow V_{\frac{\omega}{3}} \equiv Q^{\frac{\omega}{6}} \pmod{p}$. □

We next establish some results concerning the divisibility of W_{mn} by a prime p such that $p \mid C_n$.

Theorem 6.23. *Suppose p is a prime such that $p \nmid 6R\Delta$ and $p \mid C_n$. Then $p \mid W_{mn}$ if and only if $V_m(\frac{W_n}{2} - R^n, R^{2n}) \equiv -R^{mn} \pmod{p}$.*

Proof. Since $p \mid C_n$, in $\mathbb{K}$ we must have $\beta^n = \gamma^n \Rightarrow W_n = 2(\alpha^{2n}\beta^n + \beta^{2n}\alpha^n + \beta^{3n})$

and $R^n = \alpha^n\beta^{2n}$. We may then notice

$$W_n - 2R^n = 2(\alpha^{2n}\beta^n + \beta^{3n})$$

and $\beta^{3n}(\alpha^{2n}\beta^n) = \alpha^{2n}\beta^{4n} = R^{2n}$. Further, since $\beta^{mn} = \gamma^{mn}$, we have

$$W_{mn} - 2R^{mn} = 2((\alpha^{2n}\beta^n)^m + (\beta^{3n})^m).$$

Note that $V_m(\frac{W_n}{2} - R^n, R^{2n}) = \alpha'^m + \beta'^m$, where $\alpha' = \alpha^{2n}\beta^n$, $\beta' = \beta^{3n}$. It follows that

$$W_{mn} - 2R^{mn} = 2V_m(\frac{W_n}{2} - R^n, R^{2n}).$$

Thus $p \mid W_{mn}$ if and only if $V_m(\frac{W_n}{2} - R^n, R^{2n}) \equiv -R^{mn} \pmod{p}$.

□

Corollary 6.23.1. *Suppose p is a prime such that $p \nmid 6R\Delta$, $W_n \equiv 6R^n \pmod{p}$ and $C_n \equiv 0 \pmod{p}$, then $W_{mn} \equiv 6R^{mn} \pmod{p}$.*

Proof. We know that

$$W_{mn} \equiv 2R^{mn} + 2V_m(\frac{W_n - 2R^n}{2}, R^{2n}) \pmod{p}.$$

Now $\frac{W_n - 2R^n}{2} \equiv \frac{6R^n - 2R^n}{2} = 2R^n \pmod{p}$ and $V_m(2S, S^2) = 2S^m$. By letting $S = 2R^{mn}$ we get

$$W_{mn} \equiv 2R^{mn} + 2(2R^{mn}) = 6R^{mn} \pmod{p}.$$

□

Corollary 6.23.2. *Suppose p is a prime such that $p \nmid 6R\Delta$, $W_n \equiv -2R^n \pmod{p}$ and $C_n \equiv 0 \pmod{p}$, then*

$$W_{mn} \equiv \begin{cases} -2R^{mn} \pmod{p} & \text{if } 2 \mid m \\ 6R^{mn} \pmod{p} & \text{if } 2 \nmid m. \end{cases}$$

Proof. Here $\frac{W_n - 2R^n}{2} \equiv -2R^n \pmod{p}$. Also $V_m(-2S, S^2) = 2(-1)^m S^m$. If $S = R^{mn}$ and $2 \nmid m$, then

$$W_{mn} \equiv 2R^{mn} + 2(-2R^{mn}) \equiv -2R^{mn} \pmod{p}.$$

Leaving S the same, but with $2 \mid m$, we have

$$W_{mn} \equiv 2R^{mn} + 2(2R^{mn}) \equiv 6R^{mn} \pmod{p}.$$

□

Theorem 6.24. *Let p be an S prime or a Q prime. If $p \mid C_n$ and*

$$\Delta' = \left(\frac{W_n}{2} - R^n\right)^2 - 4R^{2n},$$

then $(\frac{\Delta'}{p}) = 1$ or 0.

Proof. If p is an S prime, we have $\beta^n = \gamma^n$ in $\mathbb{K}$ $(= \mathbb{F}_p)$ since $p \mid C_n$. So $\Delta' = (\frac{W_n}{2} - R^n)^2 - 4R^{2n} = (\alpha^{2n}\beta^n + \beta^{3n})^2 - 4(\alpha^n\beta^{2n})^2 = \alpha^{4n}\beta^{2n} + 2\alpha^{2n}\beta^{4n} + \beta^{6n} - 4\alpha^{2n}\beta^{4n} = \alpha^{4n}\beta^{2n} - 2\alpha^{2n}\beta^{4n} + \beta^{6n} = (\alpha^{2n}\beta^n - \beta^{3n})^2$. Thus $(\frac{\Delta'}{p}) = 1, 0$.

If p is a Q prime, we must have $\beta, \gamma \in \mathbb{F}_{p^2}$, $\alpha \in \mathbb{F}_p$.

If $p \mid C_n$ and we have $\alpha^n = \beta^n \Rightarrow \alpha^n = \beta^n = \gamma^n \Rightarrow W_n = 6R^n \Rightarrow \Delta' = (2R^n)^2 - 4R^{2n} = 0$.

If $p \mid C_n$ and we have $\beta^n = \gamma^n$, then $\Delta' = (\alpha^{2n}\beta^n - \beta^{3n})^2$. Now $(\alpha^{2n}\beta^n - \beta^{3n})^p = \alpha^{2pn}\beta^{pn} - \beta^{3pn} = \alpha^{2n}\gamma^n - \gamma^{3n} = \alpha^{2n}\beta^n - \beta^{3n}$. Thus $\alpha^{2n}\beta^n - \beta^{3n} \in \mathbb{F}_p$ and $(\frac{\Delta'}{p}) = 1$.

□

Theorem 6.25. *If p is a prime such that $p \mid C_n$, $p \nmid 6R\Delta$ and $(\frac{\Delta'}{p}) = 0$, there is no value of m such that $p \mid W_{mn}$.*

Proof. If $(\frac{\Delta'}{p}) = 0$, then $p \mid \Delta'$. Also, $p \mid \Delta' \Rightarrow p \mid (\frac{W_n}{2} - R^n)^2 - 4R^{2n} \Rightarrow (\frac{W_n}{2} - R^n)^2 \equiv 4R^{2n} \pmod{p} \Rightarrow \frac{W_n}{2} - R^n \equiv \pm 2R^n \pmod{p} \Rightarrow W_n \equiv 6R^n$ or $W_n \equiv -2R^n$. Thus, by Corollaries 6.23.1 and 6.23.2 we have $p \nmid W_{mn}$ for all m.

□

If p is a Q prime, we know that $p \mid C_{p+1}$. Suppose $p \mid E_\rho$, $\rho > 1$, ρ minimal, then we must have $p \equiv 1 \pmod{3}$ by Theorem 6.2 and $r \mid \rho \Rightarrow \rho = kr$, where r is the rank of apparition of p in $\{C_n\}$. Also $r \mid p+1$ and if $k > 1$, by the minimality of ρ we must have $p \nmid W_r$.

Put

$$P' \equiv W_r/2 - R^r \quad \text{and} \quad Q' \equiv R^{2r} \pmod{p}.$$

Then $p \mid W_\rho \Leftrightarrow V_k(P', Q') \equiv -R^{kr} \pmod{p}$ by Theorem 6.21. Let ω' be the rank of apparition of p in $U_n(P', Q')$. Now $V_k(P', Q') \equiv -R^{kr} \Rightarrow V_k^2(P', Q') \equiv Q'^k \pmod{p} \Rightarrow p \mid U_{3k}(P', Q')$, $p \nmid U_k(P', Q')$. The least possible value for k is $\omega'/3$ and $\omega' | \frac{p-1}{2}$, as $(\frac{Q'}{p}) = 1$. But if $V_{\omega'/3}(P', Q') \equiv R^{kr} \pmod{p}$, where $k = \omega'/3$, then $V_{2\omega'/3}(P', Q') \equiv -R^{2kr} \pmod{p}$. Hence $k = \omega'/3$ or $2\omega'/3$. In either event, $k \mid \frac{p-1}{3}$.

Theorem 6.26. *If p is a Q prime and ρ exists, then $\rho = kr$, where $r \mid p+1$ and $k \mid \frac{p-1}{3}$.*

As mentioned earlier, if $\rho(p)$ exists, then $\rho = kr$, where r is some rank of apparition of p in $\{C_n\}$. If p is an S prime, then $kr \mid \frac{p-1}{3} \Rightarrow k \mid \frac{p-1}{3r}$. If we put $P' \equiv \frac{W_r}{2} - R^r$, $Q' \equiv R^{2r} \pmod{p}$, then k exists if and only if $(\frac{\Delta'}{p}) = 1$ and $3 \mid \omega'$, where ω' is the rank of apparition of p in $U_n(P', Q')$. Furthermore, $k = \omega'/3$ or $2\omega'/3$. In particular by Theorem 6.22 we know that $k = 2\omega'/3$ if $2 \mid \omega'$.

The theorem below provides an analogue to both Theorems 2.16 and 2.17. Rather than consider highest powers of 2 as in the Lucas case, we consider powers of 3.

Theorem 6.27. *Suppose* $(r_1, r_2) = 1$ *and* $r_1 \mid E_m$, $r_2 \mid E_n$. *If* $3^\mu \mid\mid m$ *and* $3^\mu \mid\mid n$ $(\mu \geq 0)$, *then*

$$r_1 r_2 \mid E_{[m,n]}.$$

If $3^\mu \mid\mid m$ *and* $3^\nu \mid\mid n$ *and* $\mu \neq \nu$, *then* $r_1 r_2 \nmid E_s$ *for any* $s \in \mathbb{Z}$.

Proof. When $3^\mu \mid\mid m$ and $3^\mu \mid\mid n$, we have $3^\mu \mid\mid [m, n]$. It follows that $3 \nmid \frac{[n,m]}{n}$ and $3 \nmid \frac{[n,m]}{m}$. Thus $r_1 \mid E_{[m,n]}$ and $r_2 \mid E_{[m,n]}$ by Corollary 6.14.1. Since $(r_1, r_2) = 1$ we get $r_1 r_2 \mid E_{[m,n]}$.

Now suppose that $3^\mu \mid\mid m$ and $3^\nu \mid\mid n$ and $\mu \neq \nu$. Put $\rho_1 = \rho(r_1)$ and $\rho_2 = \rho(r_2)$. We know that $\rho_1 \mid m$ and $\rho_2 \mid n$. Also, $3 \nmid \frac{m}{\rho_1}$, $3 \nmid \frac{n}{\rho_2} \Rightarrow 3^\mu \mid\mid \rho_1$, $3^\nu \mid\mid \rho_2$.

Suppose for some $s \in \mathbb{Z}$ we get $r_1 r_2 \mid E_s$. Then $\rho_1 \mid s$, $\rho_2 \mid s$ and $3 \nmid \frac{s}{\rho_1}$, $3 \nmid \frac{s}{\rho_2}$. But then $3^\mu \mid\mid s$ and $3^\nu \mid\mid s$ and hence $\mu = \nu$ which is contrary to our assumptions. □

Put $\rho = \rho(3)$, $3^\mu \mid\mid E_\rho$. If $\rho \nmid n$ then $3 \nmid E_n$. If $\rho \mid n$ and $3 \mid \frac{n}{\rho}$, then $3 \mid\mid E_n$ by Corollary 6.10.3. If $\rho \mid n$ and $3 \nmid \frac{n}{\rho}$, then $3^\mu \mid\mid E_n$ by Corollary 6.10.4.

The next theorems parallel Theorems 2.18 and 2.19.

Theorem 6.28. *Let* $3^\mu \mid\mid m$, $3^\nu \mid\mid n$. *If* $\mu = \nu$, *then*

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

Proof. Let $(W_m, C_m, W_n, C_n) = 2^\lambda 3^\kappa d$ such that $(d, 6) = 1$. Since $3^\mu \mid\mid m$ and $3^\mu \mid\mid n$, we have $3 \nmid \frac{m}{(m,n)}$, $3 \nmid \frac{n}{(m,n)}$. Hence $E_{(m,n)} \mid E_m$ and $E_{(m,n)} \mid E_n$; consequently, $E_{(m,n)} \mid 2^\lambda 3^\kappa d$.

We know that $\lambda = 0$ or 1 by Theorem 4.5. If $\lambda = 0$, then $\rho(2) \nmid m$ or $\rho(2) \nmid n \Rightarrow \rho(2) \nmid (m,n) \Rightarrow 2 \nmid E_{(m,n)}$. If $\lambda = 1$, then $\rho(2) \mid m$, $\rho(2) \mid n \Rightarrow \rho(2) \mid (m,n) \Rightarrow 2 \mid E_{(m,n)}$. Thus $E_{(m,n)} = 2^{\lambda}3^{\kappa'}d'$ where $(d',6) = 1$, and $\kappa' \leq \kappa$, $d' \mid d$.

If $\kappa = 0$, then $\rho(3)$ does not exist $\Rightarrow 3 \nmid E_{(m,n)}$, or $\rho(3)$ exists and $\rho(3) \nmid m$ or $\rho(3) \nmid n \Rightarrow \rho(3) \nmid (m,n) \Rightarrow \kappa' = 0$.

If $\kappa = 1$, then $\rho = \rho(3)$ exists and $\rho \mid m$, $\rho \mid n$. Without loss of generality assume $3 \mid\mid E_n$. Let $3^{\delta} \mid\mid E_{\rho}$. If $\delta = 1$, then $3 \mid\mid 2^{\lambda}3^{\kappa'}d' \Rightarrow \kappa' = \kappa$. If $\delta > 1$, then $3 \mid \frac{m}{\rho}$, $3 \mid \frac{n}{\rho} \Rightarrow 3 \mid\mid 2^{\lambda}3^{\kappa'}d' \Rightarrow \kappa' = \kappa$.

If $\kappa > 1$, then $\rho(3^{\kappa}) \mid m$, $\rho(3^{\kappa}) \mid n$ and $3 \nmid \frac{m}{\rho(3^{\kappa})}$, $3 \nmid \frac{n}{\rho(3^{\kappa})}$. Now $\rho(3^{\kappa}) \mid (m,n)$ and $3 \nmid \frac{(m,n)}{\rho(3^{\kappa})} \Rightarrow 3^{\kappa} \mid 3^{\kappa'} \Rightarrow \kappa' \geq \kappa > 1$. Since $\kappa' \leq \kappa$, we get $\kappa = \kappa'$.

Now since $\rho(d) \mid m$ and $\rho(d) \mid n$, we must have $\rho(d) \mid (m,n)$. Also, since $3 \nmid \frac{m}{\rho(d)}$ and $3 \nmid \frac{n}{\rho(d)}$, we get $3 \nmid \frac{(m,n)}{\rho(d)}$. Hence, $d \mid E_{(m,n)}$ and so $d \mid d'$. Thus $d = d'$. □

Theorem 6.29. *If $3^{\mu} \mid\mid m$, $3^{\nu} \mid\mid n$ and $\nu \neq \mu$, then*

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

Proof. If we are given $p \mid (E_m, E_n)$ and $(p,6) = 1$, then $\rho(p) \mid m$ and $\rho(p) \mid n$. Since $3 \nmid \frac{m}{\rho(p)}$ and $3 \nmid \frac{n}{\rho(p)}$, we get $3^{\mu} \mid\mid \rho(p)$, $3^{\nu} \mid\mid \rho(p)$, which is impossible. If $3^{\lambda} \mid (E_m, E_n)$ and $\lambda > 1$, then $\rho(3^{\lambda}) \mid m$, $\rho(3^{\lambda}) \mid n$. Also, $3 \nmid \frac{m}{\rho(3^{\lambda})}$, $3 \nmid \frac{n}{\rho(3^{\lambda})} \Rightarrow 3^{\mu} \mid\mid \rho(3^{\lambda})$ and $3^{\nu} \mid\mid \rho(3^{\lambda})$. Again, this is impossible. Further, by Theorem 4.5, if $2^{\lambda} \mid\mid (E_m, E_n)$, then $\lambda \in \{0,1\}$. □

Thus, we also have a result comparable to Theorem 2.19.

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

Theorem 6.30. *If $p \nmid 2\Delta Q$, then*

$$p \mid U_{\frac{T(p)}{2}} \Leftrightarrow Q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$
$$p \mid V_{\frac{T(p)}{2}} \Leftrightarrow Q^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

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

By using Theorems 6.2, 6.16, 6.18, 5.14, 5.15, and 5.17, we can prove our analogue of this result.

Theorem 6.31. *Suppose p is a prime such that $p \nmid \Delta R$ and $p \equiv 1 \pmod{3}$. Let $T(p) = p^2 - 1$ if p splits in $\mathbb{Q}(\alpha)$ and $T(p) = p^2 + p + 1$ otherwise. If p is a Q or I prime, then*

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

If p is an S prime, then

$$p \mid D_{\frac{T(p)}{3}} \Leftrightarrow R^{\frac{p-1}{3}} \equiv 1 \pmod{p} \quad \textit{and} \quad p \mid C_{\frac{p-1}{3}}.$$

Also, if $T(p) = p^2 - 1$, then

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

If $T(p) = p^2 + p + 1$, then

$$p \nmid E_{\frac{T(p)}{3}}.$$

Chapter 7

Primality Testing

7.1 An Analogue of Lucas' Fundamental Theorem

As we have seen in Chapter 1, one of Lucas' main purposes in attempting to extend his functions was to find new primality tests. In this chapter we will explore how the W_n and C_n functions can be used for producing such tests. We will first develop some analogues of Theorem 2.22 of Chapter 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

$$1 > \frac{1}{5^{2k}} + 2\left(\frac{7}{10}\right)^k \quad \text{for } k \geq 2.$$

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

$$\begin{aligned} 1 \;&>\; \prod_{i=1}^{k} \frac{1}{r_i^2} + 2\prod_{i=1}^{k}\left(\frac{1+\frac{1}{r_i}+\frac{1}{r_i^2}}{2}\right) \\ &\Rightarrow \left(\prod_{i=1}^{k} r_i^2\right) > \left(\prod_{i=1}^{k} r_i^2\right)\left(\prod_{i=1}^{k}\frac{1}{r_i^2}\right) + \left(\prod_{i=1}^{k} r_i^2\right)\left(2\prod_{i=1}^{k}\left(\frac{1+\frac{1}{r_i}+\frac{1}{r_i^2}}{2}\right)\right) \\ &\Rightarrow \left(\prod_{i=1}^{k} r_i^2\right) - 1 > 2\prod_{i=1}^{k}\left(\frac{r_i^2+r_i+1}{2}\right). \end{aligned}$$

□

Theorem 7.2. *Let N be an integer such that $(N,6)=1$. If $N \mid D_{N^2-1}$, $N \nmid D_{\frac{N^2-1}{q}}$ for all primes q such that $q \mid N^2-1$ and $(D_{\frac{N^2-1}{q'}}, N) = 1$ 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 $\omega(N) \mid \frac{N^2-1}{q} \Rightarrow N \mid D_{\frac{N^2-1}{q}}$, 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, since $N \mid D_{N^2-1}$, then by equation (5.1) and the fact $2 \nmid N$, we must have $(N,R)=1$. We know by Theorem 5.11 that

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

Since $(p_i, \omega(N)) = 1$ and by Theorem 5.10 $\omega(p_i^{\alpha_i}) = p_i^{\nu}\omega(p_i)$, we must have

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

Let p be any 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 $\omega(p) \nmid \frac{N^2-1}{q'} \Rightarrow q' \mid \omega(p)$. Hence

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

Now by Corollary 5.6.1, for $k \geq 2$ we have,

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

we get

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

which is impossible by the previous lemma.

If $k = 1$, then $N = p^\alpha$ and by Theorem 5.10 $\omega(N) = \omega(p^\alpha) = p^\nu \omega(p) \Rightarrow N^2 - 1 = \omega(p)$, since $(p, N^2-1) = 1$. 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 $(N, 6) = 1$. If $N \mid D_{N^2+N+1}$ and $N \nmid D_{\frac{N^2+N+1}{q}}$ for each prime divisor q of N^2+N+1 and $(D_{\frac{N^2+N+1}{q'}}, N) = 1$ for some prime divisor q' of N^2+N+1, then N is a prime.*

We have proved our analogue of Theorem 2.22.

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

The difficulty in providing this as a complete analogue to Lucas' result is the need to involve the prime q', which is not needed in Theorem 2.22. This is because $2 \mid N \pm 1$ and $2 \mid p_i \pm 1$, and any proof of Theorem 2.22 makes use of these observations. In what follows next, we will modify Theorems 7.2 and 7.3 to eliminate the need for q' in certain cases.

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

$$W_m \equiv -3R^m, \;\; \Delta C_m^2 \equiv -27R^{2m} \pmod{p}.$$

We also have a result for an arbitrary modulus.

Lemma 7.5. *Let* $(N, 6) = 1$. *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 $N \mid W_{3n} - 6R^{3n} \Rightarrow N \mid D_{3n}$. Now since $(W_n, C_n, R) \mid 2$ by Lemma 4.6 and $(N, 6) = 1$ we have $(N, R) = 1 \Rightarrow N \nmid C_n$. □

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

Theorem 7.6. *If 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 $N \mid D_{T(N)}$, $N \nmid D_{\frac{T(N)}{q}}$ for all prime divisors of $T(N)$. By our earlier reasoning we have $\omega(N) = T(N)$. Also, since $(T(N), N) = 1$,

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

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, by Corollary 4.2.1 we can only have $p = 2$, which is not possible because N is odd. Thus, $(N, R) = 1$. 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 $(N, 6\Delta R) = 1$. 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 $(\frac{-3\Delta}{p}) = 1$. If p is an I prime, then $\omega(p) \mid p^2 + p + 1$, $(\frac{\Delta}{p}) = 1$ and $(\frac{-3}{p}) = 1$, 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,

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

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

Notice that $3 \mid T(N)$ when $T(N) = N^2 - 1$ and $3 \mid T(N)$ 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' precept that the primality of N 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 N is odd and let m be any positive integer such that $(m, N) = 1$. If $N \mid C_{mn}/C_n$, then $(N, D_n) = 1$.*

Proof. Suppose p is any prime divisor of D_n and N. Since $p \mid C_n$ and $p \mid W_n - 6R^n$, we see by our results in Section 4.4, in particular equation (5.4), we have that

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

It follows that since $p \nmid m$ and $p \nmid R$ ($(D_n, R) \mid 2$), 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 2.23.1.

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

Proof. Since $(T(N), N) = 1$, we have $(q, N) = 1$. By Lemma 7.7 we know that if p is any prime divisor of N, then $(N, D_{\frac{T(N)}{q}}) = 1$. Thus, $N \nmid D_{\frac{T(N)}{q}}$ for all prime divisors q of $T(N)$ and $(N, D_{\frac{T(N)}{q'}}) = 1$ for some (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 by using the methods of Section 3.6.

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 section, 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.*

Proof. If N is composite, there must be a prime p such that $p \mid N$ and $p \leq \sqrt{N}$. Also, since $\omega(p) \mid N^2 + N + 1$, we must have $\omega(p) \mid tL$. Certainly $\omega(p) \neq 1$ and since $p \nmid D_t$, $\omega(p) \nmid t$. It follows that since $\omega(p) \mid tL$ and $\omega(p) \nmid t$, we must have $L \mid \omega(p)$. Now, $\omega(p) \leq p^2 + p + 1$ by Corollary 5.6.1; hence

$$p^2 + p + 1 \geq L = \frac{N^2 + N + 1}{t}$$

or

$$t(p^2 + p + 1) \geq N^2 + N + 1 = (N + \sqrt{N} + 1)(N - \sqrt{N} + 1).$$

Since $p \leq \sqrt{N}$ and $N + \sqrt{N} + 1 \geq p^2 + p + 1$, we get $t \geq N - \sqrt{N} + 1$, a contradiction.

□

Corollary 7.9.1. *If N is odd, $N \equiv 1 \pmod 3$, $L = (N^2 + N + 1)/3$ is a prime, $(N, D_3) = 1$, and $N \mid D_{N^2+N+1}$, then N is a prime.*

Proof. If N is composite, then $N \geq 5^2$ and $3 < 5^2 - 5 + 1$. □

We also have the following result.

Theorem 7.10. *Let $N^2 + N + 1 = tL$, where L is a prime. If $L > t^2 + t + 1$, $(N, D_t) = 1$ and $N \mid D_{N^2+N+1}$, then N is a prime.*

Proof. From our proof of Theorem 7.9 we know that if p is any prime divisor of N, then $L \mid \omega(p)$. Thus, $N^2 + N + 1 \mid t\omega(p)$. Hence, if N is composite, then $N = pr$ $(r > 1)$ and

$$p^2r^2 + pr + 1 \leq t\omega(p) \leq t(p^2 + p + 1);$$

hence, $r < t$. Now let q be any prime divisor of r. Then since $q \mid N$ we have $L \mid \omega(q)$ and

$$t^2 + t + 1 < L \leq q^2 + q + 1.$$

It follows that $r \geq q > t$, a contradiction. □

Now, suppose 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 7.11. *If $N = tS + u$, where $S \geq 2$ and $N > 4$, we have $t < N - \sqrt{N} + 1$.*

Proof. Since

$$N - \sqrt{N} + 1 = \frac{1}{4}(2\sqrt{N} - 1)^2 + \frac{3}{4},$$

we see that $N - \sqrt{N} + 1$ is an increasing function of N for $N > 0$. Thus, since $N \geq 2t + u > 0$, we get

$$N - \sqrt{N} + 1 \geq 2t + u - \sqrt{2t + u} + 1.$$

If $u = 0, -1, -2$, then $1 \leq t \leq 3$ and $N - \sqrt{N} + 1 > 4 - 2 + 1 > t$. If $u \neq 0, -1, -2$, then $(u + 1)^2 \geq 4$ and

$$(u + 1)^4 \geq 4(u + 1)^2 > 2u^2 + 3u + 2 = 2t + u.$$

Thus,

$$(u + 1)^2 > \sqrt{2t + u} \quad \text{and hence} \quad 2t + u - \sqrt{2t + u} > t.$$

□

From Theorems 7.9 and 7.11 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, 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], [Leh58]) that if N is a prime and

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

where p is a prime ($\equiv 1 \pmod 3$), $4p = r^2 + 27s^2$ 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

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

Notice that since $(pr, N) = 1$, there always exists some x such that $(pr + xN, -3p) = 1$; hence, the fact that $(-3p, pr) = p \neq 1$ does not have any affect on the validity of our results. We have proved the following theorem.

Theorem 7.12. *Let $L = tS^2 + (2u+1)S + 1$ be a prime and put $N = tS + u$. Suppose $(N, 6) = 1$, 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 $(N, prs) = 1$. If we put*

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

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

Corollary 7.12.1. *Let $2 \nmid S$, $L = 3S^2 - 3S + 1$ be a prime and 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 $(N, prs) = 1$, then N is a prime if and only if $N \mid D_{N^2+N+1}$, where

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

Proof. This follows easily from the theorem by putting $u = -2$ and noting that

$$\Delta \equiv 27(4p^3 - p^2r^2) \pmod{N},$$

$$W_1 = PQ - 3R \equiv -3pr \pmod{N},$$

$$4C_3 = \Delta + 3W_1^2 \equiv -4(27p^3) \pmod{N}.$$

Hence, $(C_3, N) = 1$. □

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. 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

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

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 $S = FG$, 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 7.13. *If $L = tS^2+(2u+1)S+1$ ($t = u^2+u+1$), $S = FG$ and all the prime factors of L have the form $kF+1$, then L is a prime when $F > tG^2 + |2u+1|G + 2$.*

Proof. Suppose L is composite. We must have

$$L = (k_1F + 1)(k_2F + 1),$$

where k_1, $k_2 \geq 1$. Hence,

$$tS^2 + (2u + 1)S = k_1k_2F^2 + (k_1 + k_2)F,$$
$$tSG + (2u + 1)G = k_1k_2F + k_1 + k_2$$

and

$$(tG^2 - k_1k_2)F = k_1 + k_2 - (2u + 1)G.$$

If $tG^2 - k_1k_2 = 0$, then

$$(k_1 - k_2)^2 = (k_1 + k_2)^2 - 4k_1k_2 = (2u + 1)^2G^2 - 4tG^2 = -3G^2,$$

which is impossible; hence $|tG^2 - k_1k_2| \geq 1$. Also, since k_1, $k_2 \geq 1$, we get $(k_1 - 1)(k_2 - 1) \geq 0$ and hence $k_1k_2 \geq k_1 + k_2 - 1$. Now

$$\begin{aligned} |tG^2 - k_1k_2|F &\leq k_1 + k_2 + |2u + 1|G \leq k_1k_2 + 1 + |2u + 1|G \\ &= k_1k_2 - tG^2 + tG^2 + |2u + 1|G + 1; \end{aligned}$$

hence,

$$F \leq tG^2 + |2u + 1|G + 2,$$

which is impossible. □

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

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

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. In the table below we provide all instances for various values of u ($-500 \leq u \leq 500$) and $n \leq 1000$ such that both L_n and N_n are prime.

Table 7.1: Values of u such that L_n and N_n are both prime ($n \leq 1000$)

n	u	n	u
1	3, -3, -5, 13, 25, 31, -33, 37, -39, 55, -57,	41	-27, 111, -141
	-71, 79, -87 -159, 181, -183, 219, -221, -243,	43	-173
	255, -255, 279, -281, 289, -291, 307, 325, 333,	46	-449
	-353, -369, 375, -395, -423, -435, -495	51	273
2	-11, 31, 55, 115, -191, -221, 271, 361	53	-53, 267, -267
3	-3, 7, 19, 25, -33, 39, -51, -65, 79, 105, 117, 177,	55	25, 87, -327, 475,
	-231, 259, -401, 483, 499	56	307, -419
4	-5,31, 223, 277, -323, 367, 415	57	217, 361, 483
5	3,-17, 19, 39, -39, -45, -65, 73, -95, -101,	58	-221
	129, -137, -153, 165, 207, -233, 295, -297,	61	475
	-323, 339, -389, 417, 463, 481	65	-195
6	-65, 145, 259, -311	69	-21, 415
7	9, -15, -95, 109, -243, 297, -297, 457, 459, -477	70	-5
8	-179, -209, -263, -395	72	361
9	9,-65, 91, -227, 397, 471	73	447
10	-5, 349	74	169
11	13, 15, 25, 87, -111, 159, 199, 285, 309, -381	75	499
12	-119, 205, 271	77	39
13	25,-33, -285, 325, 349, -449	79	-227
14	199,-281, -359,439	83	-251
15	9, 25, 39, 105, -105, -107, 235, 313, 397, 415, -471	84	-35
16	-89,277, -389, -395, -407	95	-65
17	61, 73, -135, -141, 255, 321, 481	96	-233
18	-101	121	27
19	-123, -221, -255, -311, 487	123	-467
20	31,-185,-269	137	-297
21	-17, 81,-149, -413, 445	140	193
22	-215, 319	143	403
23	127, 129, 265, -275, -323, -335, -401, -437	207	123
25	-267, -309, 499	211	-141
27	39,-161	231	163
28	181	360	-467
30	235	399	117
32	187, -209	407	237
35	-381, 463	417	-257
38	361	533	-407
40	-365	819	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. We illustrate this rarity in the next table, we provide those few values of n for which L_n and N_n are both prime for all $n < 1000$.

Table 7.2: Prime pairs for specific choices of u and q

u	q	L_n	N_n	$n < 1000$
2	3	$7 \cdot 3^{2n} + 5 \cdot 3^n + 1$	$7 \cdot 3^n + 2$	1
-2	3	$3 \cdot 3^{2n} - 3 \cdot 3^n + 1$	$3 \cdot 3^n - 2$	1, 4, 5
-2	5	$3 \cdot 5^{2n} - 3 \cdot 5^n + 1$	$3 \cdot 5^n - 2$	1, 2
-2	7	$3 \cdot 7^{2n} - 3 \cdot 7^n + 1$	$3 \cdot 7^n - 2$	1
-2	11	$3 \cdot 11^{2n} - 3 \cdot 11^n + 1$	$3 \cdot 11^n - 2$	1, 7
3	2	$13 \cdot 2^{2n} + 7 \cdot 2^n + 1$	$13 \cdot 2^n + 3$	1, 5
-3	2	$7 \cdot 2^{2n} - 5 \cdot 2^n + 1$	$7 \cdot 2^n - 3$	1, 3
-4	3	$13 \cdot 3^{2n} - 7 \cdot 3^n + 1$	$13 \cdot 3^n - 4$	2
6	5	$43 \cdot 5^{2n} + 13 \cdot 5^n + 1$	$43 \cdot 5^n + 6$	15
6	11	$43 \cdot 11^{2n} + 13 \cdot 11^n + 1$	$43 \cdot 11^n + 6$	1
8	3	$73 \cdot 3^{2n} + 17 \cdot 3^n + 1$	$73 \cdot 3^n + 8$	1
12	5	$157 \cdot 5^{2n} + 25 \cdot 5^n + 1$	$157 \cdot 5^n + 12$	1
14	3	$211 \cdot 3^{2n} + 29 \cdot 3^n + 1$	$211 \cdot 3^n + 14$	1, 17
15	2	$241 \cdot 2^{2n} + 31 \cdot 2^n + 1$	$241 \cdot 2^n + 15$	11
-15	2	$211 \cdot 2^{2n} - 29 \cdot 2^n + 1$	$211 \cdot 2^n - 15$	7
-18	11	$307 \cdot 11^{2n} - 35 \cdot 11^n + 1$	$307 \cdot 11^n - 18$	11
-21	2	$421 \cdot 2^{2n} - 41 \cdot 2^n + 1$	$421 \cdot 2^n - 21$	69
27	2	$757 \cdot 2^{2n} + 55 \cdot 2^n + 1$	$757 \cdot 2^n + 27$	121
-28	3	$757 \cdot 3^{2n} - 55 \cdot 3^n + 1$	$757 \cdot 3^n - 28$	3, 9

In the particular case of $u = -2$, $q = 3$, row 2 of Table 7.2, 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

$$b^{L_n - 1} \equiv 1 \pmod{L_n} \quad \text{and} \quad (b^{\frac{L_n - 1}{3}} - 1, L_n) = 1, \tag{7.1}$$

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 (7.1) we have

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

If ω 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 7.12.1 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 2.24, except for the necessity condition.

Theorem 7.14. *Let $N = A3^n - 1$, where $2 \mid A$, $A < 3^n$, $n \geq 2$ and $(N, R) = 1$. If*

$$N \mid C_{N+1}/C_{\frac{N+1}{3}},$$

then N is prime.

Proof. Let p be any prime divisor of N. Since $p \mid C_{N+1}$, we must have some rank of apparition $r(p)$ in $\{C_n\}$ such that $r(p) \mid N+1$. Also, since

$$4C_{N+1}/C_{\frac{N+1}{3}} = \Delta C^2_{\frac{N+1}{3}} + 3W^2_{\frac{N+1}{3}},$$

we see that if $p \mid C_{\frac{N+1}{3}}$, then $p \mid W_{\frac{N+1}{3}}$. Hence $p \mid E_{\frac{N+1}{3}}$ and by Theorem 6.7, we know that $p \equiv 1 \pmod{3^n}$. If $p \nmid C_{\frac{N+1}{3}}$, then $r(p) \nmid \frac{N+1}{3}$. It follows that $3^n \mid r(p)$. If $p \mid \Delta$, then $r(p) \mid p$ or $p-1$ and the first case is impossible, as $p \mid N$ and $r(p) \mid N+1 \Rightarrow r(p) \nmid p$. If p is an I prime, then $r(p) \mid p^2+p+1$, but this is impossible because $9 \nmid p^2+p+1$. If p is an S prime or a Q prime, then $r(p) \mid p^2-1$ and $p \equiv \pm 1 \pmod{3^n}$. Thus, any prime divisor of N must be at least as large as $2 \cdot 3^n - 1$. Since $(2 \cdot 3^n - 1)^2 > N$, N must be a 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 2.25. We begin with the following theorem.

Theorem 7.15. *Let p be an odd prime such that $p \equiv -1 \pmod{3}$. Then there exist P, Q, R such that p is a Q prime if and only if*

$$P \equiv a + \mathrm{Tr}(\lambda), \quad Q \equiv a\,\mathrm{Tr}(\lambda) + \mathrm{N}(\lambda), \quad R \equiv a\,\mathrm{N}(\lambda) \pmod{p},$$

where $a \in \mathbb{Z}$, $\lambda = r_1 + r_2\rho \in \mathbb{Z}[\rho]$, $\rho^2 + \rho + 1 = 0$ and $p \nmid ar_2\,\mathrm{N}(\lambda)$.

Proof. Suppose P, Q, R satisfy the conditions of the theorem. Then clearly

$$\begin{aligned}\Delta &\equiv (a-\lambda)^2(a-\bar{\lambda})^2(\lambda-\bar{\lambda})^2 \\ &= N(a-\lambda)^2 r_2^2(\rho-\rho^2)^2 \\ &= -3m^2 \pmod{p},\end{aligned}$$

where $m \in \mathbb{Z}$. Since $p \equiv -1 \pmod 3$ and $p \nmid ar_2\,\mathrm{N}(\lambda)$, we cannot have $p \mid m$. Thus

$$\left(\frac{\Delta}{p}\right) = \left(\frac{-3m^2}{p}\right) = \left(\frac{-3}{p}\right) = -1.$$

Since $p \nmid 6R\Delta$, p is a Q prime for $f(x) = x^3 - Px^2 + Qx - R$.

Next, suppose that p is a Q prime for $f(x) = x^3 - Px^2 + Qx - R$. Then $\mathbb{F}_{p^2}$ is the splitting field of $f(x)$ in $\mathbb{F}_p[x]$. Let α, β, γ be the zeros of $f(x)$ in $\mathbb{F}_{p^2}$, where $\alpha^p = \alpha$, $\beta^p = \gamma \neq \beta = \gamma^p$. Since $\mathbb{F}_{p^2}^* = \langle\theta\rangle$ for some suitable $\theta \in \mathbb{F}_{p^2}$, we put $\zeta = \theta^{\frac{p^2-1}{3}}$ and note that $\zeta^2 + \zeta + 1 = 0$. Now since $p \equiv -1 \pmod 3$,

$$\left(\frac{\beta-\gamma}{\zeta-\zeta^2}\right)^p = \frac{\gamma-\beta}{\zeta^2-\zeta} = \frac{\beta-\gamma}{\zeta-\zeta^2}.$$

Hence $\frac{\beta-\gamma}{\zeta-\zeta^2} \in \mathbb{F}_p$. If we put

$$a \equiv \alpha, \;\; b \equiv \frac{\beta-\gamma}{\zeta-\zeta^2} \not\equiv 0, \;\; c \equiv \beta+\gamma = P-\alpha \equiv P-a \pmod{p},$$

then

$$\beta = \frac{b+c}{2} + b\zeta, \;\; \gamma = \frac{b+c}{2} + b\zeta^2.$$

Putting $r_1 \equiv (b+c)/2 \pmod p$, $r_2 \equiv b \pmod p$ we see that

$$P \equiv a + \mathrm{Tr}(\lambda), \;\; Q \equiv a\,\mathrm{Tr}(\lambda) + \mathrm{N}(\lambda), \;\; R \equiv a\,\mathrm{N}(\lambda) \pmod{p},$$

for $\lambda = r_1 + r_2\rho$, $p \nmid r_2$. Since $p \nmid R$, we must also have $p \nmid a\,\mathrm{N}(\lambda)$. □

We can now present our analogue of Theorem 2.25.

Theorem 7.16. *Let p be an odd prime such that $p \equiv -1 \pmod 3$. If P, Q, R satisfy the conditions of Theorem 7.15 and $\left(\frac{\lambda}{p}\right)_3 \neq 1$, then*

$$p \mid C_{p+1}/C_{\frac{p+1}{3}}.$$

Proof. By Theorem 7.15, we know that p is a Q prime and therefore $p \mid C_{p+1}$. Let α, β, γ be the zeros of $f(x)$ in $\mathbb{F}_{p^2}$, where $\alpha^p = \alpha$, $\beta^p = \gamma \neq \beta = \gamma^p$. Since $\lambda^{\frac{p^2-1}{3}} \not\equiv 1 \pmod p$, we may assume with no loss of generality that $\beta^{\frac{p^2-1}{3}} \neq 1$ in $\mathbb{F}_{p^2}$. Since

$$\beta^{\frac{p^2-1}{3}} = (\beta^{p-1})^{\frac{p+1}{3}} = \left(\frac{\gamma}{\beta}\right)^{\frac{p+1}{3}},$$

we have $\beta^{\frac{p+1}{3}} \neq \gamma^{\frac{p+1}{3}}$. Also, since

$$\beta^{p\frac{p+1}{3}} = \gamma^{\frac{p+1}{3}} \neq \beta^{\frac{p+1}{3}},$$

we cannot have $\alpha^{\frac{p+1}{3}} = \beta^{\frac{p+1}{3}}$ because $\beta^{\frac{p+1}{3}} \notin \mathbb{F}_p$. Similarly $\alpha^{\frac{p+1}{3}} \neq \gamma^{\frac{p+1}{3}}$. It follows that $C_{\frac{p+1}{3}} \neq 0$ in $\mathbb{F}_{p^2}$ or $p \nmid C_{\frac{p+1}{3}}$. Hence $p \mid C_{p+1}/C_{\frac{p+1}{3}}$. □

By combining Theorems 7.14 and 7.16 we get the following necessary and sufficient condition for $N = A3^n - 1$ ($2 \mid A$, $A < 3^n$) to be prime.

Theorem 7.17. *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 $\lambda = r_1 + r_2\rho$ ($\rho^2 + \rho + 1 = 0$) be a primary prime divisor of q in $\mathbb{Z}[\rho]$ and suppose that $N \nmid r_2$. Let

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

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

$$N \mid C_{p+1}/C_{\frac{p+1}{3}}.$$

Proof. Since $(N, R) = 1$, we know by Theorem 7.14 that N is a prime if

$$N \mid C_{p+1}/C_{\frac{p+1}{3}}.$$

Next, suppose that N is a prime. We know that

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

and since λ is a primary prime divisor of q, we have by the cubic reciprocity law

$$\left(\frac{N}{\lambda}\right)_3 \neq 1 \Rightarrow \left(\frac{\lambda}{N}\right)_3 \neq 1.$$

Thus, $N \mid C_{p+1}/C_{\frac{p+1}{3}}$ by Theorem 7.16. □

7.5 Primality Test

We may now use Theorem 7.17 to produce a primality test, somewhat similar to the Lucas and Lehmer test for numbers of the form $A2^n - 1$, for numbers of the form $A3^n - 1$. Of course, this test is not as practical as that of [Wil72b], but it would have been of some interest to Lucas that C_n could be used to produce such a test. Let $m \in \mathbb{Z}^+$ such that $(m, 2R) = 1$. Compute

$$S_0 \equiv \frac{W_n}{2R^n} \pmod{m} \quad \text{and} \quad R_0 \equiv \frac{\Delta C_n^2}{4R^{2n}} \pmod{m}$$

and define

$$S_i \equiv \frac{W_{3^i n}}{2R^{n3^i}} \pmod{m} \quad \text{and} \quad R_i \equiv \frac{\Delta C_{3^i n}^2}{4R^{2n3^i}} \pmod{m}.$$

Notice then

$$\begin{aligned}
S_{i+1} &= \frac{1}{2}R^{-n3^{i+1}}W_{3^{i+1}n} = \frac{1}{2}R^{-n3^{i+1}}W_{3(3^in)} \\
&= \frac{1}{2}R^{-n3^{i+1}}\left[3\frac{\Delta C_{3^in}^2}{4}(W_{3^in}+2R^{3^in}) + \frac{W_{3^in}^3}{4} - \frac{6R^{3^in}W_{3^in}}{4} + 6R^{3^{i+1}n}\right] \\
&= \frac{1}{2}R^{-n3^{i+1}}\left[3R^{2(3^in)}R_i(2R^{3^in}S_i+2R^{3^in}) + \frac{(2R^{3^in}S_i)^3}{4} - \frac{6R^{3^in}(2R^{3^in}S_i)^2}{4} + 6R^{3^{i+1}n}\right] \\
&= \frac{1}{2}R^{-n3^{i+1}}\left[3R_iR^{3^{i+1}n}2(S_i+1) + 2R^{3^{i+1}n}S_i^3 - 6R^{3^{i+1}n}S_i^2 + 6R^{3^{i+1}n}\right] \\
&= 3R_i(S_i+1) + S_i^3 - 3S_i^2 + 3.
\end{aligned}$$

Similarly,

$$R_{i+1} = \frac{\Delta C_{3^{i+1}n}^2}{4R^{2(3^{i+1}n)}}.$$

Using Corollary 3.10.1 we have

$$C_{3^{i+1}n} = \frac{1}{4}C_{3^in}(\Delta C_{3^in}^2 + 3W_{3^in}^2).$$

Use this and the fact that

$$W_{3^in} \equiv 2R^{3^in}S_i \quad \text{and} \quad \Delta C_{3^in}^2 \equiv 4R^{2(3^in)}R_i \pmod{m}$$

to obtain

$$C_{3^{i+1}n} = \frac{1}{4}C_{3^in}(4R^{2(3^in)}R_i + 3(2R^{3^in}S_i)^2).$$

This yields

$$\begin{aligned}
C_{3^{i+1}n}^2 &= \frac{1}{4}C_{3^in}^2\frac{1}{4}(4R^{2(3^in)}R_i + 3(2R^{3^in}S_i)^2)^2 = \frac{C_{3^in}^2}{4}\frac{1}{4}(4R^{2(3^in)}R_i + 12R^{2(3^in)}S_i^2)^2 \\
&= \frac{C_{3^in}^2}{4}\frac{1}{4}(4R^{2(3^in)}(R_i+3S_i^2))^2 = \frac{C_{3^in}^2}{4}4R^{4(3^in)}(R_i+3S_i^2)^2.
\end{aligned}$$

We manipulate this as follows:

$$\frac{\Delta C_{3^{i+1}n}^2}{4} = \frac{\Delta C_{3^in}^2R^{4(3^in)}}{4}(R_i+3S_i^2)^2.$$

So then we get

$$\frac{\Delta C^2_{3^{i+1}n}}{4R^{2(3^{i+1})n}} = \frac{\Delta C^2_{3^in}R^{4(3^in)}}{4R^{2(3^{i+1})n}}(R_i + 3S_i^2)^2.$$

Thus

$$\begin{aligned} R_{i+1} &= \frac{\Delta C^2_{3^in}R^{4(3^in)}}{4R^{6(3^i)n}}(R_i + 3S_i^2)^2 = \frac{\Delta C^2_{3^in}}{4R^{2(3^i)n}}(R_i + 3S_i^2)^2 \\ &= R_i(R_i + 3S_i^2)^2. \end{aligned}$$

We can now employ these observations to produce our primality test. If we satisfy the conditions of Theorem 7.17 where $N = 3^nA - 1$ and set

$$S_0 \equiv \frac{W_A}{2R^A} \pmod N \quad \text{and} \quad R_0 \equiv \frac{\Delta C_A^2}{4R^{2A}} \pmod N,$$

then

$$S_i \equiv \frac{W_{3^iA}}{2R^{3^iA}} \pmod N \quad \text{and} \quad R_i \equiv \frac{\Delta C^2_{3^iA}}{4R^{2(3^iA)}} \pmod N.$$

We can produce the sequence $\{S_i\}$ and $\{R_i\} \pmod N$ as follows:

$$S_{i+1} \equiv 3R_i(S_i+1)+S_i^3-3S_i^2+3 \pmod N \quad \text{and} \quad R_{i+1} \equiv R_i(R_i+3S_i^2) \pmod N.$$

Then N is a prime if and only if $R_{n-1} \equiv -3S_{n-1}^2 \pmod N$.

Chapter 8

Conclusion

8.1 Main Result

The purpose of this thesis 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 functions that displays a number of pleasing similarities with Lucas' original work. The main tools in Lucas' investigation of his functions were the multiplication formulas (2.14) and (2.15). The multiplication formulas, proved in Section 3.5, 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, as described in Sections 4.4, 4.5, 5.2, 5.3, 6.2, and 6.3, have analogues in our extension. Most remarkably, the extension relies on the use of only two functions[1], despite the fact that you would expect three for the cubic case. Further, when restricted to the quadratic case, our generalization in Section 3.3 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' own goal in generalizing his sequences was to find and implement new primality tests, Theorem 7.17 and the primality test of Section 7.5 based on it stand out. 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

[1]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.

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 2.22, which Lucas refered to as his fundamental theorem. It should be stated, 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.

8.2 Improvements

In terms of what might be done to refine or improve the results of the thesis, it would by satisfying to have more elementary proofs of Theorems 4.18 and 4.19. As it stands, both proofs use facts from algebraic number theory, and these are the only two instances where such powerful tools are required. However, some key results from Serret's *Cours d'algèbre supérieure* Vol. II [Ser79] allow for the desired elementary alternate proof of Theorem 4.18. For the details, the interested reader is directed to Appendix A. In fact, Lucas was familiar with Serret's work, so if Lucas had proved this result, it is imaginable that he would have used the methods seen in Appendix A.

It would also be interesting to develop further the law of repetition for $\{D_n\}$ so that it more closely matches the Lucas case, where if p is a prime and for $\lambda > 0$, we have $p^\lambda \neq 2$ and $p^\lambda \mid\mid U_m$, then $p^{\lambda+\mu} \mid\mid U_{mnp^\mu}$ when $p \nmid n$ and $\mu \geq 0$. This is how the law of repetition is presented for $\{U_n\}$ in Chapter 4 of [Wil98].

8.3 Future Work

Beyond the thesis itself, work could be done to try to use $\{C_n\}$ and $\{W_n\}$ to implement an RSA-type cryptosystem. Peter Smith's LUC [Smi93][2], a well-known example of such a cryptosystem using the Lucas functions, provides the motivation for this. It might also be possible to use $\{C_n\}$ and $\{W_n\}$ to perform a Diffie-Hellman-like key exchange.

There is also, of course, the possibility of exploring the idea of a quartic extension as mentioned by Lucas. For such an extension, C_n and W_n would be as described early in Section 3.3. Despite being an interesting problem, we would expect it to be difficult to work with the quartic case due to the number of terms involved in the recurrences.

[2]See [BBL95] for some useful comments concerning LUC.

Bibliography

[AS82] W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), 255–300.

[Bac93] E. Bach, *Comments on Peter Smith's LUC public-key encryption system*, University of Wisconsin, 1993.

[BBL95] D. Bleichenbacher, W. Bosma, and A. K. Lenstra, *Some remarks on Lucas-based cryptosystems*, Advances in Cryptology—CRYPTO '95 (Santa Barbara, CA, 1995), Lecture Notes in Comput. Sci., vol. 963, Springer, Berlin, 1995, pp. 386–396.

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

[Bel30] ———, *Letter to Professor D. Harkin from E. T. Bell*, A copy in possession of Hugh Williams, 1930.

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

[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.

[BPvdP90] J. P. Bézivin, A. Pethő, and A. J. van der Poorten, *A full characterization of divisibility sequences*, Amer. J. Math. **112** (1990), 985–1001.

[Cai08] C. Cailler, *Congruences du troisième degré*, L'Enseignement mathém. **10** (1908), 474–487.

[Car13] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Annals of Mathematics **15** (1913), 30–70.

[Car20] ———, *On sequences of integers defined by recurrence relations*, Quarterly Journal of Mathematics **48** (1920), 343–372.

[CP01] R. Crandall and C. Pomerance, *Prime Numbers - A Computational Perspective*, Springer-Verlag, New York, 2001.

[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.

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

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

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

[Eng31] H. T. Engstrom, *On sequences defined by linear recurrence relations*, Trans. Amer. Math. Soc. **33** (1931), 210–218.

[gim] *Great Internet Mersenne Prime Search*, `www.mersenne.org`.

[Gra47] C. Graves, *On algebraic triplets*, Proc. Royal Irish Acad. **3** (1847), 51–54, 57–64, 80–84, 105–108.

[Hal36] M. Hall, *Divisibility sequences of the third order*, Amer. Journal of Math. **58** (1936), 577–584.

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

[Hil98] D. Hilbert, *The Theory of Algebraic Number Fields*, Springer-Verlag, Berlin, 1998, Translated from the German and with a preface by Iain T. Adamson, With an introduction by Franz Lemmermeyer and Norbert Schappacher.

[Isk] B. Iskra, *The prime pages*, `http://primes.utm.edu/bios/page.php?id=484`.

[Lai96] C.-A. Laisant, *Question 744*, L'Intermédiaire des Mathématitiens **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. of the Amer. Math. Soc. **33** (1927), 327–340.

[Leh30] ———, *An extended theory of Lucas' functions*, Ann. of Math. **31** (1930), 419–448.

[Leh33] ———, *Factorization of certain cyclotomic functions*, ibid **33** (1933), 461–479.

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

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

[Leh68] ———, *Use of Pierce functions for a primality test*, unpublished notes, 1968.

[Leh71] ———, *The economics of number theoretic computation*, Academic press (1971), 1–9.

[Leh93] ———, *The mathematical work of Morgan Ward*, Math. Comp. **61** (1993), 307–312.

[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] ———, *Théorie des fonctions numériques simplement périodiques*, American Journal of Math **1** (1878), 189–240, 289–321.

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

[Luc91a] ———, *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] ———, *Théorie des nombres*, Gauthier-Villars, Paris, 1891.

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

[Men62] N. S. Mendelsohn, *Congruence relationships for integral recurrences*, Can. 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] ———, *On the computation of cube roots modulo p*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., 2004, pp. 293–304.

[Pie16] T. A. Pierce, *The numerical factors of the arithmetic forms* $\prod^n(1 \pm \alpha_i^m)$, Annals of Math. **2** (1916), 53–64.

[Rib89] P. Ribenboim, *The Book of Prime Number Records*, 2 ed., Springer-Verlag, 1989.

[Ros00] K. H. Rosen, *Elementary Number Theory and its Applications*, 4 ed., Addison-Wesley, 2000.

[Ser79] J. A. Serret, *Cours d'Algèbre Supérieure*, vol. II, Gauthier-Villars, 1879.

[SHWL96] P. Stevenhagen and Jr. H. W. Lenstra, *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), 26–37.

[Smi93] P. Smith, *LUC public-key encryption - a secure alternative to RSA*, Dr. Dobb's Journal (1993), 44–51.

[Sze96] G. Szekeres, *High order pseudoprimes in primality testing*, Paul Erdös Is Eighty, Bolyai Soc. Math. Stud. **2** (1996), 451–458.

[War31a] M. Ward, *The algebra of recurring series*, Annals of Math. (2) **32** (1931), 1–9.

[War31b] ———, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), 153–165.

[War31c] ———, *The distribution of residues in a sequence satisfying a linear recurrence relation*, Trans. Amer. Math. Soc. **33** (1931), 166–190.

[War33] ———, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. **35** (1933), 600–628.

[War36] ———, *A calculus of sequences*, Amer. Journal of Math. **58** (1936), 255–266.

[War37] ———, *Linear divisibility sequences*, Trans. Amer. Math. Soc. **41** (1937), 276–286.

[War38] ———, *The law of apparition of primes in a Lucasian sequence*, Trans. Amer. Math. Soc. **44** (1938), 68–86.

[War55] ———, *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] ———, *On a generalization of the Lucas function*, Acta Arith. **20** (1972), 33–52.

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

[Wil76] ———, *A generalization of Lehmer's functions*, Acta Arith. **29** (1976), 315–341.

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

[Wil98] ———, *Édouard Lucas and primality testing*, Wiley-Interscience, 1998.

[WJ76] H. C. Williams and J. S. Judd, *Some algorithms for prime testing using generalized Lehmer functions*, Math. Comp. **30** (1976), 867–886.

[WS94] H. C. Williams and J. O. Shallit, *Factoring integers before computers*, Symposia in Applied Mathematics, vol. 48, 1994, pp. 481–531.

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

Appendix A

In this appendix we provide an elementary proof of Theorem 4.18. This proof could easily have been discovered by Lucas through his admitted knowledge of Chapter III of [Ser79]. We first recapitulate some of the preliminary results in Serret's work.

Definition A.1. *Let p be a prime and let $f(x)$, $g(x) \in \mathbb{Z}[x]$. If there exist $h(x)$, $k(x) \in \mathbb{Z}[x]$ such that*

$$h(x)g(x) = f(x) + pk(x),$$

we say that $f(x)$ is divisible by $g(x)$ with respect to modulus p. *We write this as*

$$h(x)g(x) \equiv f(x) \pmod{p}.$$

Definition A.2. *If $f(x) \in \mathbb{Z}[x]$, $f(x)$ is monic and $f(x)$ is not divisible by any $g(x) \in \mathbb{Z}[x]$ with respect to modulus p, we say that $f(x)$ is* irreducible with respect to p.

Theorem A.3. *If $g(x)$, $h(x) \in \mathbb{Z}[x]$, $g(x)$, $h(x)$ have no common divisor (of degree ≥ 1) with respect to the prime modulus p, then there exist $Y(x)$, $Z(x) \in \mathbb{Z}[x]$ such that*

$$Y(x)h(x) - Z(x)g(x) \equiv 1 \pmod{p}.$$

The next result does not appear explicitly in [Ser79], but it would have been easy for Lucas to derive because its proof is entirely analogous to that of the elementary number theory result which states that if a, b, $c \in \mathbb{Z}$, $(a, b) = 1$, $a \mid c$ and $b \mid c$, then $ab \mid c$. This is proved by Lucas on p. 340 in [Luc91b]. The proof of Theorem A.4 would follow in exactly the same manner by using Theorem A.3.

Theorem A.4. *If $f(x)$, $g(x)$, $h(x) \in \mathbb{Z}[x]$, $g(x)$ and $h(x)$ have no common divisor (of degree ≥ 1) with respect to the prime modulus p, and $g(x)$, $h(x)$ are both divisors of $f(x)$ modulo p, then $g(x)h(x)$ is a divisor of $f(x)$ with respect to the modulus p.*

The next result (Theorem I in Section 346 of [Ser79]) is most important for our subsequent work. We give it in a somewhat different form from Serret's results, but Serret certainly establishes it in his proof of Theorem I.

Theorem A.5. *Let $f(x) \in \mathbb{Z}[x]$ be irreducible with respect to a prime modulus p and of degree ν. Then $f(x)$ is a divisor of $x^{p^\nu - 1} - 1$ with respect to the modulus p.*

We now suppose that $f(x) = x^3 - Px^2 + Qx - R$ and p is a prime such that $p \nmid 6\Delta R$. We know that when p is an S prime we have

$$f(x) \equiv f_1(x) f_2(x) f_3(x) \pmod{p},$$

where $f_1(x)$, $f_2(x)$, $f_3(x) \in \mathbb{Z}[x]$ are each monic of degree 1 and, because $p \nmid \Delta$, have no common divisor with respect to p. If p is a Q prime, then

$$f(x) \equiv f_1(x) f_2(x) \pmod{p},$$

where $f_1(x)$, $f_2(x) \in \mathbb{Z}[x]$; $f_1(x)$, $f_2(x)$ are monic and irreducible with respect to the modulus p, $\deg f_1(x) = 1$, $\deg f_2(x) = 2$. Finally, if p is an I prime, then $f(x)$ is irreducible with respect to the modulus p.

It is now easy to prove, by making use of Theorems A.4 and A.5, that $f(x)$ is a divisor of $x^{p^\mu - 1} - 1$ with respect to the modulus p, where $\mu = 1$ when p is an S prime, $\mu = 2$ when p is a Q prime, and $\mu = 3$ when p is an I prime. Putting $m = p^\mu - 1$, we have

$$x^m - 1 = f(x)g(x) + ph(x)$$

for some $g(x)$, $h(x) \in \mathbb{Z}[x]$. Putting $x = \alpha$, β, γ, where α, β, $\gamma \in \mathbb{C}$ are the zeros of $f(x)$, we get

$$\alpha^m - 1 = ph(\alpha),$$

$$\beta^m - 1 = ph(\beta),$$

$$\gamma^m - 1 = ph(\gamma),$$

from which it follows that

$$\alpha^m - \beta^m = p(h(\alpha) - h(\beta)),$$

$$\beta^m - \gamma^m = p(h(\beta) - h(\gamma)),$$

$$\gamma^m - \alpha^m = p(h(\gamma) - h(\alpha)).$$

Hence

$$\begin{aligned} \Delta C_m^2 &= (\alpha^m - \beta^m)^2(\beta^m - \gamma^m)^2(\gamma^m - \alpha^m)^2 \\ &= p^6 S(\alpha, \beta, \gamma) \end{aligned}$$

where,

$$S(x, y, z) = (h(x) - h(y))^2(h(y) - h(z))^2(h(z) - h(x))^2.$$

Since $S(x, y, z)$ is a symmetric polynomial in $\mathbb{Z}[x, y, z]$, we must have $S(\alpha, \beta, \gamma) \in \mathbb{Z}$ by the fundamental theorem of symmetric polynomials, and therefore $p^3 \mid C_m$. Also

$$\begin{aligned} W_m - 6R^m &= \alpha^m(\beta^m - \gamma^m)^2 + \beta^m(\gamma^m - \alpha^m)^2 + \gamma^m(\alpha^m - \beta^m)^2 \\ &= p^2 T(\alpha, \beta, \gamma), \end{aligned}$$

where

$$\begin{aligned} T(x, y, z) &= (h(y) - h(z))^2 + (h(z) - h(x))^2 + (h(x) - h(y))^2 \\ &\quad + p[h(x)(h(y) - h(z))^2 + h(y)(h(z) - h(x))^2 + h(z)(h(x) - h(y))^2]. \end{aligned}$$

Since $T(x, y, z)$ is also a symmetric polynomial in $\mathbb{Z}[x, y, z]$, we must have $T(\alpha, \beta, \gamma) \in \mathbb{Z}$ and $p^2 \mid W_m - 6R^m$.

We are now able to present another proof of Theorem 4.18.

Theorem A.6. *If $p \nmid 6\Delta R$ and $p \mid C_n$, $p \mid W_n - 6R^n$, then $p^3 \mid C_n$ and $p^2 \mid W_n - 6R^n$.*

Proof. Let $\omega = \omega(p)$. Clearly ω exists and ω divides both n and m by Theorem 5.5. From the proof of Theorem 5.1, we know that

$$C_m/C_\omega \equiv (m/\omega)^3 R^{m-\omega} \pmod{p}.$$

Thus, since $p \nmid m$, we get $p \nmid C_m/C_\omega \Rightarrow p^3 \mid C_\omega \Rightarrow p^3 \mid C_n$. Also from the proof of Theorem 5.1, we have

$$W_m - 6R^m \equiv (m/\omega)^2 R^m (W_\omega - 6R^\omega) \pmod{p^2};$$

thus, we get $p^2 \mid W_\omega - 6R^\omega$. Furthermore,

$$W_n - 6R^n \equiv (n/\omega)^2 R^n (W_\omega - 6R^\omega) \pmod{p^2}$$

means that $p^2 \mid W_n - 6R^n$. □

Although this proof requires Theorems 5.1 and 5.5, these results did not require the result of Theorem 4.18 in their respective proofs.