

https://dspace.org/

The proof of the Primitive Divisor Theorem

Sias, Mark Anthony

2016

http://hdl.handle.net/10539/21293

Sias, Mark Anthony (2016) The proof of the Primitive Divisor Theorem, University of Witwatersrand, Johannesburg, <http://wiredspace.wits.ac.za/handle/10539/21293>

Downloaded from a DSpace repository. https://dspace.org/



The Proof of the Primitive Divisor Theorem

by

© *Mark Sias*

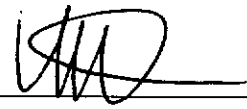
A research project submitted
in fulfillment of the requirements
for the degree of Master of Science

School of Mathematics
University of the Witwatersrand

May 2016

Declaration

I declare that this Dissertation is my own, unaided work. It is being submitted for the degree of Master of Science at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at any other University.



_____ (Signature of candidate)

28 TH day of MAY 20 16 in BRAAMFONTEIN

Abstract

This dissertation provides the main results leading up to its primary aim, the proof of the Primitive Divisor Theorem, by appealing to an eclectic potpourri of mathematical machinery. The employment of binary recurrent sequences with related results is crucial to the approach adopted. The various forms in which the theorem manifests are attributed, among others, to K. Zsigmondy, P.D. Carmichael, and Y. Bilu, G. Hanrot and P.M. Voutier. The proof is confined to instances where the roots of the characteristic polynomial are integers, and when the roots are reals. This dissertation culminates in the resolution of a Diophantine equation which serves as an application of the Primitive Divisor Theorem that is attributable to Carmichael.

Acknowledgements

I dedicate this dissertation to my fiance, June, for her labour of love and her unremitting motivation, both of which serve to inspire me, in spite of seemingly insurmountable odds. Additionally, I extend my sincere gratitude to my supervisor, Professor Florian Luca, for his support and guidance. Due appreciation is also expressed to my friend Sizwe Mdakane for his belief in my ability to complete the project successfully. The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged as well. Opinions expressed and conclusions arrived at, are those of the author and are not to be attributed necessarily to the NRF.

Contents

Declaration ii

Abstract iii

Acknowledgements iv

1 Introduction 1

1.1 Preliminaries 2

1.2 Binary recurrent sequences 5

1.2.1 The Fibonacci and Lucas sequences 6

1.2.2 Binary recurrences associated to Pell equations with $N = \pm 1$. 7

1.2.3 Binary recurrences associated to Pell equations with $N \neq \pm 1$. 8

2 The Proof of Zsigmondy's Theorem 10

2.1 Introduction 10

2.2 Cyclotomic Polynomials 10

2.3 Lucas Sequences 12

2.3.1 Definitions and Examples 12

2.3.2 Prime factors of terms of Lucas sequences 13

2.4 Zsigmondy's Theorem 14

3 The Proof of Carmichael's Theorem 19

3.1 Introduction 19

4 Two applications of Carmichael's Theorem **24**

4.1 Introduction 24

4.2 Application 1 25

4.3 Application 2 25

Chapter 1

Introduction

In a paper published in 1904, Birkhoff and Vandiver [2] formulated an elementary proof stating that, for every fixed positive integer n, the set of primes $p \equiv 1 \pmod{n}$ is infinite. Three approaches, viz. Binary Recurrent Sequences, or Continued Fractions or Linear Forms in Logarithms may be adopted to achieve this proof.

The importance of recurrence sequences hardly needs explanation since its study is clearly of inherent interest and has been a pivotal aspect of number theory for some years, see [6]. Furthermore, recurrence sequences arise in virtually every field of mathematics and computer science, for example, the theoretical aspects of power series which represent rational functions, pseudo-random number generators, k-regular and automatic sequences and cellular automata, see [6]. Linear recurrences are also formed by sequences of solutions of Diophantine equations, see [6]. In many interesting instances a diverse range of power series, such as the zeta-functions of algebraic varieties of finite fields, generating functions that arise from group theory, dynamical zeta functions of many dynamical systems, Hilbert series and commutative algebra, Poincare series, and closely related series, are all known to be rational, see [6]. The coefficients of the series representing such functions are linear recurrence sequences, see [6].

In addition, recurrence sequences enter many spheres of the mathematical sciences in

a broader sense (which includes applied mathematics and applied computer science), see [6]. For instance, we have that quite a large number of systems of orthogonal polynomials, including the Tchebychev polynomials and the Dickson polynomials, which are their finite field counterparts, satisfy recurrence relations, see [6]. Linear recurrence sequences also play a key role in approximation theory and cryptography and have also found application in time series analysis and computer graphics, see [6].

In chapter 1, we furnish the reader with some basic definitions and results from Algebra and Number Theory that will serve to aid understanding of the dissertation's primary aim. Chapter 2 provides an alternative proof of Zsigmondy's Theorem via a cursory glance at Cyclotomic Polynomials, Lucas sequences, and Prime factors of terms of Lucas sequences. Chapter 3 puts forth an alternative proof of Carmichael's Theorem, while the last chapter, (chapter 4), contains two applications of this theorem.

1.1 Preliminaries

In this section, some fundamental notions from Algebra and Number Theory, that arise frequently, will be defined. We will define only those notions which are relevant to this dissertation and thus refer the reader to [4], [6], [7], [8], [11], [12], [13] and [14].

Definition 1.1.1 (see [4]). *Let $F[x]$ denote a polynomial ring over the field F. The polynomial $f(x) \in F[x]$ is **irreducible** if $\deg(f(x)) > 0$ and given any polynomial $p(x) \in F[x]$, then either $f(x)$ is relatively prime to $p(x)$ or $f(x) \mid p(x)$.*

Definition 1.1.2 (see [14]). *For any $n > 0$,*

$$\phi(n) = \textit{number of integers less than or equal to } n \textit{ and relatively prime to } n.$$

*The function ϕ is called the **Euler phi** function.*

Definition 1.1.3 (see [14]). *Suppose that p is an odd prime and $p \nmid a$. If the congruence*

$$x^2 \equiv a \pmod{p}$$

is soluble then a is called a ***quadratic residue modulo*** *p, and if it has no solution, then a is called a* ***quadratic nonresidue modulo*** *p.*

Definition 1.1.4 (see [14]). *Let p be an odd prime and a an integer; the* ***Legendre symbol*** *(a/p) is defined by*

(1) $(a/p) = 1$ if a is a quadratic residue mod p,

(2) $(a/p) = -1$ if a is a quadratic nonresidue mod p.

(3) $(a/p) = 0$ if $p \mid a$.

Definition 1.1.5 (see [7]). *Let E_m be the set of κ_m^j, $j = 0, 1, 2, \ldots, m-1$ where κ_m is the complex number $\kappa_m = \cos(2\pi/m) + i\sin(2\pi/m)$. The elements of E_m are called the* ***mth roots of unity****.*

Definition 1.1.6 (see [12]). *If $\alpha \in \mathbb{C}$ is a root of a monic, integral polynomial of degree k, viz. a root of a polynomial of the form*

$$f(x) = \sum_{j=0}^{k} a_j x^j \in \mathbb{Z}[x], a_k = 1$$

(where $\mathbb{Z}[x]$ denotes the ring of polynomials with integer coefficients), which is irreducible over $\mathbb{Q}$, then α is called an ***algebraic integer*** *of degree k.*

Definition 1.1.7 (see [12]). *An* ***algebraic number****, β, of degree $k \in \mathbb{N}$ is a root of a monic polynomial in $\mathbb{Q}[x]$ of degree k and not the root of any polynomial in $\mathbb{Q}[x]$ of degree less than k. Stated equivalently, an* ***algebraic number*** *is the root of an irreducible polynomial of degree k over $\mathbb{Q}$.*

Definition 1.1.8 (see [12]). *An* ***algebraic number field****, or simply* ***number field****, has the form $F = \mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_n) \subseteq \mathbb{C}$ for $n \in \mathbb{N}$ where β_j for $j = 1, 2, \ldots, n$ are algebraic numbers.*

Definition 1.1.9. *Given any integer sequence $S = (S_n)_{n\geq 1}$, we define a* ***primitive divisor*** *of the term $S_n(\neq 0)$ to be a divisor of S_n that is coprime to every nonzero term S_m with $m < n$. Any prime factor of a primitive divisor is called a* ***primitive prime divisor.***

The following example serves to illustrate the definition of a primitive divisor.

Example 1.1.10. We note that the Mersenne sequence $M = (M_n) = 2^n - 1$ for $n = 1, 2, \ldots$ contains infinitely many primes. Factoring the first few terms of the Mersenne sequence reveals several primitive divisors, as displayed in Table 1.1. We note that M_6 has no primitive divisor, but each of the previous terms has at least one.

Table 1.1: The Primitive divisors of (M_n).

n	M_n	Factorisation
2	3	3
3	7	7
4	15	$3 \cdot 5$
5	31	31
6	63	$3^2 \cdot 7$
7	127	127
8	255	$3 \cdot 5 \cdot 17$
9	511	$7 \cdot 73$

1.2 Binary recurrent sequences

This section will primarily contain the main definitions and propositions/theorems, which will serve to pave the way for the main result.

Definition 1.2.1 (see [13]). *Let $k \geq 1$ be an integer. A sequence $(w_n)_{n\geq 0} \subseteq \mathbb{C}$ is called* ***linearly recurrent of order*** *k if the recurrence*

$$w_{n+k} = a_1 w_{n+k-1} + a_2 w_{n+k-2} + \ldots + a_k w_n \tag{1.2.1}$$

holds for all $n \geq 0$ with $a_1, \ldots, a_k \in \mathbb{C}$.

Definition 1.2.2 (see [6]). *Suppose that $a_k \neq 0$. If $a_1, \ldots, a_k \in \mathbb{Z}$ and $w_0, \ldots, w_{k-1} \in \mathbb{Z}$, then, by induction on n, we find that w_n is an integer for all $n \geq 0$. The polynomial*

$$f(X) = X^k - a_1 X^{k-1} - \cdots - a_k \in \mathbb{C}[X]$$

is called the ***characteristic polynomial*** *of $(w_n)_{n\geq 0}$.*

Suppose that $f(X) = \prod_{i=1}^{s} (X - \alpha_i)^{\sigma_i}$, where $\alpha_1, \ldots, \alpha_s$ are the distinct roots of $f(X)$ with multiplicities $\sigma_1, \ldots, \sigma_s$, respectively.

Proposition 1.2.3 (see [11]). *Suppose that $f(X) \in \mathbb{Z}[X]$ has k distinct roots. Then there exist constants $c_1, \ldots, c_k \in \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ such that the formula*

$$w_n = \sum_{i=1}^{k} c_i \alpha_i^n \tag{1.2.2}$$

holds for all $n \geq 0$.

Note that for $k = 2$, the sequence $(w_n)_{n\geq 0}$ is called **binary recurrent**. Here we observe that its characteristic polynomial is of the form

$$f(X) = X^2 - a_1 X - a_2 = (X - \alpha_1)(X - \alpha_2).$$

Definition 1.2.4 (see [8]). *A binary recurrent sequence $(w_n)_{n\geq 0}$ whose general term is given by equation (1.2.2), with $k = 2$, is referred to as* ***nondegenerate*** *if $c_1 c_2 \alpha_1 \alpha_2 \neq 0$ and $\frac{\alpha_1}{\alpha_2}$ is not a root of unity.*

To illuminate the foregone discussion we proceed to some examples of binary recurrent sequences, viz. the Fibonacci and Lucas sequences.

1.2.1 The Fibonacci and Lucas sequences

The Fibonacci sequence $(F_n)_{n\geq 0}$ is given by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. The characteristic polynomial is $f(X) = X^2 - X - 1 = (X - \alpha_1)(X - \alpha_2)$. The formula for finding the roots of a quadratic equation yields $\alpha_1 = (1 + \sqrt{5})/2$ and $\alpha_2 = (1 - \sqrt{5})/2$. To find the constants c_1 and c_2 from equation (1.2.2), we ascribe to n the values 0 and 1. Upon solving the two equations that arise we get $c_1 = 1/\sqrt{5}, c_2 = -1/\sqrt{5}$. As $(\alpha_1 - \alpha_2) = \sqrt{5}$, we may write

$$F_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} \tag{1.2.1.1}$$

for $n \geq 0$. Closely related to the Fibonacci sequence is the Lucas sequence $(L_n)_{n\geq 0}$ given by $L_0 = 2, L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$. Its characteristic polynomial is that of the Fibonacci sequence; hence there exist two constants d_1 and d_2 such that

$$L_n = d_1\alpha_1^n + d_2\alpha_2^n$$

for all $n \geq 0$. Assigning the values 0 and 1 to n we find $d_1 = d_2 = 1$. Thus,

$$L_n = \alpha_1^n + \alpha_2^n \tag{1.2.1.2}$$

for all $n \geq 0$. By utilising equation (1.2.1.1) and equation (1.2.1.2), one can easily derive various formulae which involve F_n and L_n. In particular, it can be readily verified that

$$L_n^2 - 5F_n^2 = 4(-1)^n$$

for all $n \geq 0$ by noting that $\alpha_1\alpha_2 = -1$ and $(\alpha_1 - \alpha_2)^2 = 5$.

1.2.2 Binary recurrences associated to Pell equations with $N = \pm 1$

The Diophantine equation $x^2 - dy^2 = 1$, usually known as Pell's equation, is of considerable importance in number theory. For $d > 1$ an integer which is not a perfect square, let (x_1, y_1) be the minimal solution in positive integers of the equation

$$x^2 - dy^2 = \pm 1. \tag{1.2.2.1}$$

It is known that (x_1, y_1) exists, see [14].

We let $\chi = x_1 + \sqrt{d}y_1$ and $\gamma = x_1 - \sqrt{d}y_1$. From the theory of Pell equations, all positive integer solutions (x, y) of equation (1.2.2.1) are of the form $(x, y) = (x_m, y_m)$ for some positive integer m, where

$$x_m + \sqrt{d}y_m = (x_1 + \sqrt{d}y_1)^m = \chi^m,$$

see [14]. By conjugating the above relation, we have

$$x_m - \sqrt{d}y_m = (x_1 - \sqrt{d}y_1)^m = \gamma^m.$$

Hence,

$$x_m = \frac{\chi^m + \gamma^m}{2} \quad \text{and} \quad y_m = \frac{\chi^m - \gamma^m}{2\sqrt{d}} \quad \text{for all } m \geq 1. \tag{1.2.2.2}$$

Putting $(x_0, y_0) = (1, 0)$ so that equation (1.2.2.2) holds with $m = 0$ as well, turns out to be quite useful. It is evident that $(x_m)_{m\geq 0}$ and $(y_m)_{m\geq 0}$ are binary recurrent sequences with characteristic polynomial

$$\begin{aligned} f(X) &= X^2 - a_1X - a_2 \\ &= (X - \chi)(X - \gamma) \\ &= X^2 - (\chi + \gamma)X + \chi\gamma \\ &= X^2 - 2x_1X \pm 1. \end{aligned}$$

1.2.3 Binary recurrences associated to Pell equations with $N \neq \pm 1$

The notion of the "continued fraction" and that of a "convergent" are required, in order to comprehend, to some extent, the material that follows. Hence, it is appropriate to state the relevant definitions and results in this regard.

Definition 1.2.5 (see [14]). *A **continued fraction** is an expression of the form*

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots}}}$$

with either a finite or infinite number of entries q_i.

We let $[q_0, q_1, \ldots]$ denote the above expression.

Theorem 1.2.6 (see [14]). *Let $q_0, q_1, \ldots$ be a finite ($k+3$ elements) or infinite sequence of positive integers, with the exception that q_0 can be zero, and let a_n and b_n be given by*

$$a_0 = q_0, \quad a_1 = q_0 q_1 + 1, \quad a_{n+2} = a_{n+1} q_{n+2} + a_n, \quad b_0 = 1, \quad b_1 = q_1, \quad b_{n+2} = b_{n+1} q_{n+2} + b_n,$$

where $n \leq k$ in the finite case. If θ is a real number greater than 1, then

(1) $[q_0, \ldots, q_n, \theta] = \frac{\theta a_n + a_{n-1}}{\theta b_n + b_{n-1}}$ *provided* $n > 0$.

(2) $[q_0, \ldots, q_n] = \frac{a_n}{b_n}$.

We let $\lfloor \theta \rfloor$ denote the integer part of θ. If θ is a non-integral positive real number then $\theta = \lfloor \theta \rfloor + \frac{1}{\theta_1} = [\lfloor \theta \rfloor, \theta_1]$ for some $\theta_1 \in \mathbb{R}$, θ_1 greater than 1.

In the same manner, if $\theta_1 \notin \mathbb{Z}$, we have $\theta_1 = \lfloor \theta_1 \rfloor + \frac{1}{\theta_2} = [\lfloor \theta_1 \rfloor, \theta_2]$ for some $\theta_2 \in \mathbb{R}$, θ_2 greater than 1 and $\theta = [\lfloor \theta \rfloor, \lfloor \theta_1 \rfloor, \theta_2]$.

This process may be continued to obtain the sequence $\theta, \theta_1, \theta_2, \theta_3, \cdots$, which will terminate at θ_k if θ_k is the first integer in this sequence, and it will continue indefinitely if none of the terms in this sequence is an integer.

Definition 1.2.7 (see [14]). *Let θ be a positive real number. Using the foregone notation and the equations for the a_i and b_i for $i = 0, 1, \ldots, n$ as in Theorem 1.2.6, the rational number $\frac{a_n}{b_n}$ is called the* ***nth convergent*** *to θ provided none of*

$$\theta_0 = \theta, \theta_1, \ldots, \theta_n$$

belong to $\mathbb{Z}$ and $q_i = \lfloor \theta_i \rfloor$ for $i = 0, 1, \ldots, n$.

Let $d > 1$ be an integer which is not a perfect square and let M be a non-zero integer. Let (v, w) be a positive integer solution of the equation

$$v^2 - dw^2 = M. \tag{1.2.3.1}$$

For $0 < |M| < \sqrt{d}$, then $\frac{v}{w}$ is a convergent of $\sqrt{d}$. It can be shown that for all fixed M all the positive integer solutions (v, w), if any, belong to a finite set of binary recurrent sequences, see [13].

Chapter 2

The Proof of Zsigmondy's Theorem

2.1 Introduction

In this chapter, we provide an alternative proof of a version of the Primitive Divisor theorem by virtue of the work done by Zsigmondy [19]. Subsequent to this Birkhoff and Vandiver, independently, furnished an elementary proof stating that for n a fixed positive integer, the set of primes $p \equiv 1 \pmod{n}$ is infinite, see [5]. The notions of "cyclotomic polynomial" and "Lucas sequences" with pertinent results that will expedite the proof of the theorem, are introduced and expanded upon forthwith. For further clarification the reader may refer to [5], [7], [13] and [19].

2.2 Cyclotomic Polynomials

The family of polynomials which has the form $X^n - 1$ have the key property that their roots are exactly the nth roots of unity. It is, however, imperative to bear in mind that many of these polynomials have common factors. Consider, for example, that for any positive integers k and n, the $\gcd(X^k - 1, X^n - 1) = X^{\gcd(k,n)} - 1$. These greatest common factors show that there exist kth roots of unity which are also nth roots of unity. Defining a polynomial $\Phi_n(X)$ whose roots are all nth roots of unity,

but not kth roots of unity for all $k < n$, enables the removal of all common factors among these polynomials.

Definition 2.2.1. *The polynomial*

$$\Phi_n(X) = \prod_{\substack{d:\gcd(d,n)=1 \\ d<n}} \left(X - e^{\frac{2\pi i d}{n}}\right) \tag{2.2.1}$$

is called the nth ***cyclotomic polynomial.*** *This polynomial has degree* $\phi(n)$.

Example 2.2.2. The following equation

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{2.2.2}$$

is very important. To illustrate this, we consider the list

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$$

and write every fraction $\frac{m}{n}$ as a fraction in its simplest form $\frac{s}{d}$ with $\gcd(s,d) = 1$ and some divisor d of n. It is easily discernable that all divisors d of n arise in this manner. Furthermore, for fixed d, all s which have $1 \leq s \leq d$ and are relatively prime to d also appear. As $e^{\frac{2\pi i m}{n}} = e^{\frac{2\pi i s}{d}}$ is a root of $\Phi_d(X)$,we get equation (2.2.2). To see how this works we observe that

$$\left(\frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6}\right) = \left(\frac{1}{6}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{5}{6}, 1\right).$$

The last number 1 leads to the only root of $\Phi_1(X) = X - 1$. The number $\frac{1}{2}$ corresponds to the only root of unity of order 2, which is -1. Thus $\Phi_2(X) = X+1$. The numbers $\frac{1}{3}$ and $\frac{2}{3}$ correspond to cubic roots of unity, therefore $\Phi_3(X) = X^2 + X + 1$. Lastly, $\frac{1}{6}$ and $\frac{5}{6}$ correspond to the two roots of unity of order 6, thus $\Phi_6(X) = X^2 - X + 1$.

Proposition 2.2.3 (see [7]). *For all* $m \in \mathbb{N}$, $\Phi_m(X) \in \mathbb{Z}[X]$.

2.3 Lucas Sequences

2.3.1 Definitions and Examples

Definition 2.3.1 (see [13]). *A Lucas sequence* $\{w_n\}_{n\geq 0}$ *is a linearly recurrent sequence of order 2*

$$w_{n+2} = r_1 w_{n+1} + r_2 w_n \quad n \geq 0,$$

for r_1 *and* r_2 *positive integers such that* $\gcd(r_1, r_2) = 1$, $w_0 = 0$, $w_1 = 1$ *and the ratio* $\frac{\alpha_1}{\alpha_2}$ *of the roots* α_1, α_2 *of* $x^2 - r_1 x - r_2 = 0$ *is not a root of* 1.

Observe that $(\alpha_1, \alpha_2) = \left(\frac{r_1+\sqrt{r_1^2+4r_2}}{2}, \frac{r_1-\sqrt{r_1^2+4r_2}}{2}\right)$. Also $r_1 = \alpha_1 + \alpha_2$ and $r_2 = -\alpha_1\alpha_2$. The initial conditions lead to $w_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2}$ with $n = 0, 1, \ldots$
Note that we refer to the pair (α_1, α_2) as a Lucas pair, see [1].

The following two examples serve to illustrate the connection between Fibonacci sequences and Lucas sequences and the relationship between Pell equations and Lucas sequences.

Example 2.3.2. The Fibonacci sequence $\{F_n\}_{n\geq 0}$ is a Lucas sequence because

$$F_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} \quad ; \quad (\alpha_1, \alpha_2) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right).$$

The companion Lucas sequence $\{L_n\}_{n\geq 0}$ of the Fibonacci sequence has

$$L_n = \alpha_1^n + \alpha_2^n = \frac{F_{2n}}{F_n}.$$

Example 2.3.3. Suppose (x_m, y_m) are all positive integer solutions to the Pell equations $x^2 - dy^2 = \pm 1$ where $d > 0$ is not a perfect square. If (x_1, y_1) is the smallest such solution, then

$$x_m + y_m\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^m.$$

Let $\chi = x_1 + \sqrt{d}y_1$ and $\gamma = x_1 - \sqrt{d}y_1$. Then we have that $\chi + \gamma = 2x_1$ and $\chi\gamma = \pm 1$. We also have

$$x_m = \frac{\chi^m + \gamma^m}{2} \quad \text{and} \quad y_m = \frac{\chi^m - \gamma^m}{2\sqrt{d}}.$$

Clearly, $\left\{\frac{y_m}{y_1}\right\}_{m\geq 0}$ is the Lucas sequence with roots (α_1, α_2) and characteristic polynomial $x^2 - r_1 x - r_2$, where $r_1 = 2x_1$ and $r_2 = \pm 1$.

2.3.2 Prime factors of terms of Lucas sequences

In this section and beyond, $(w_n)_{n\geq 0}$ denotes a Lucas sequence. For the sake of convenience we set $\Delta = (\alpha_1 - \alpha_2)^2$. We collate results about the number theoretic properties of Lucas sequences. We recall that an algebraic integer is a complex number which is the root of a monic polynomial of which the coefficients are integers. The integers are algebraic integers. Naturally the same applies to products and sums of algebraic integers. The integers are the only rationals that are algebraic integers. If k is an integer and δ is an algebraic integer, we say that k divides δ if $\frac{\delta}{k}$ is an algebraic integer. The most important divisibility properties of the Lucas sequences are summed up in the propositions and lemmas below.

Proposition 2.3.4 (see [13]). *For p an odd prime number we have the following properties:*

(i) If $p \mid r_2$, then $p \nmid w_m$ for all $m \geq 1$;

(ii) If $p \mid \Delta$, then $p \mid w_p$;

(iii) If $p \nmid \Delta r_2$ and $(\Delta/p) = 1$, then $p \mid w_{p-1}$;

(iv) If p is an odd prime excluded in (i)-(iii), then $p \mid w_{p+1}$.

Proposition 2.3.5 (see [13]). *For m and n positive integers we have*

$$\gcd(w_m, w_n) = w_{\gcd(m,n)}.$$

Lemma 2.3.6 (see [13]). *Suppose that $m \mid n$ and p is a prime such that $p \mid \gcd(w_m, \frac{w_n}{w_m})$, then $p \mid \frac{n}{m}$.*

Lemma 2.3.7 (see [13]). *For p an odd prime and $p \mid w_n$, then $p \mid\mid \frac{w_{np}}{w_n}$.*

We need the following statements and definitions to further enhance understanding of the proof of Zsigmondy's theorem in the next section.

Definition 2.3.8 (see [13]). *For a prime p, let t_p be the **order of appearances** of p in $\{w_n\}_{n\geq 0}$; that is, the minimal positive integer k such that $p|w_k$. If $p \nmid w_n$ for any $n > 0$, then define $t_p = \infty$.*

Proposition 2.3.9 (see [13]). *If $p \mid w_n$ then $t_p \mid n$.*

Remark 2.3.10. *If $\eta(p)$ is the period of the Fibonacci sequence modulo p, then $\eta(p) \in \{t_p, 2t_p, 4t_p\}$.*

Theorem 2.3.11 (see [13]). *If $p \nmid \Delta r_2$, then $p \equiv \pm 1 \pmod{t_p}$.*

Definition 2.3.12 (see [13]). *$p|w_n$ is a **primitive divisor** of w_n if $t_p = n$.*

2.4 Zsigmondy's Theorem

We now have sufficient mathematical machinery to enable us to present an alternative proof to Zsigmondy's Theorem.

Theorem 2.4.1. *If the roots of the characteristic polynomial of $\{w_n\}_{n\geq 0}$ are coprime positive integers and if $n > 6$, then w_n has a primitive divisor.*

Proof. Note that the homogenisation of the polynomial

$$f(X) = a_j X^j + a_1 X^{j-1} + \cdots + a_0$$

is simply the homogeneous polynomial $f(X, Y) = a_j X^j + a_1 X^{j-1} Y + \cdots + a_0 Y^j$. We suppose that m is large and that c and d are the roots of the characterisic polynomial

of $\{w_n\}_{n\geq 0}$. We let

$$\Phi_m(X,Y) = \prod_{\substack{1\leq k\leq m\\ \gcd(k,m)=1}} (X - e^{\frac{2\pi ik}{m}}Y) \in \mathbb{Z}[X,Y]$$

be the homogenisation of the cyclotomic polynomial for m. The formula $X^m - 1 = \prod_{j|m}\Phi_j(X)$ may be homogenised to $X^m - Y^m = \prod_{j|m}\Phi_j(X,Y)$. Let $\Phi_m(c,d) = KL$, and assume that each prime p that divides L is primitive, while the primes q that divide K are not primitive. Suppose now that $p \mid K$, then $p \mid w_m$ and $p \mid w_j$, where we have some $j < m$. Suppose that $j \mid m$ (if not, substitute j by $\gcd(j,m)$). As $p \mid K \mid \Phi_m(c,d) \mid \frac{w_m}{w_j}$, where the latter divisibility relation follows from $X^m - Y^m = \prod_{r|m}\Phi_r(X,Y)$, for $(X,Y) = (c,d)$, we have that $p \mid \gcd(w_j, \frac{w_m}{w_j})$. Thus, from Lemma 2.3.6, we get that $p \mid \frac{m}{j}$ and therefore, $j \mid \frac{m}{p}$. Hence, $p \mid w_j \mid w_{m/p}$, but $K \mid \Phi_m(c,d) \mid \frac{w_m}{w_{\frac{m}{p}}}$. By invoking Lemma 2.3.7 with $j = \frac{m}{p}$, we have $p \mid\mid K$ for p odd. Now, assume that $p = 2$. When the parities of c and d are not identical or m is odd, then w_m is odd. So, in this case we must have that c and d are odd and m is even. If $2 \mid\mid m$, then $K \mid \frac{w_m}{w_2} = \frac{((c^2)^{\frac{m}{2}} - (d^2)^{\frac{m}{2}})}{(c^2-d^2)}$ is again odd, and if $4 \mid m$, then $K \mid \frac{w_m}{w_{\frac{m}{2}}} = c^{\frac{m}{2}} + d^{\frac{m}{2}} = (c^{\frac{m}{4}})^2 + (d^{\frac{m}{4}})^2$. But c and d are odd, thus, it must be the case that the above sum of two odd squares is congruent to 2 modulo 4. This implies that the exponent of 2 in the factorisation of K does not exceed 1 either. Thus, K is square free and $K \mid m$. Note that by the Principle of Inclusion and Exclusion,

$$\Phi_m(c,d) = \frac{c^m - d^m}{\prod_{p|m}(c^{\frac{m}{p}} - d^{\frac{m}{p}})} \frac{\prod_{\substack{p<q\\ pq|m}}(c^{\frac{m}{pq}} - d^{\frac{m}{pq}})}{\prod_{\substack{p<q<s\\ pqs|m}}(c^{\frac{m}{pqs}} - d^{\frac{m}{pqs}})} \cdots . \tag{2.4.1}$$

As $c^j > c^j - d^j = (c-d)(c^{j-1} + \ldots + d^{j-1}) \geq c^{j-1}$, it implies that a lower bound on $\Phi_m(c,d)$ can be established by substituting each factor $c^j - d^j$ in the numerator of equation (2.4.1) by c^{j-1} and each factor in the denominator of equation (2.4.1) by c^j. Therefore, we find

$$\Phi_m(c,d) \geq c^{m - \sum_{p|m}\frac{m}{p} + \sum_{pq|m}\frac{m}{pq} - \cdots - 2^{\omega(m)} - 1} \geq c^{\phi(m) - 2^{\omega(m)} - 1},$$

where $\omega(m)$ is the number of distinct prime factors of m. Since $K \leq m$, we have $L \geq \frac{c^{\phi(m)-2^{\omega(m)-1}}}{m}$. Hence, for $L = 1$, we have $\phi(m) - 2^{\omega(m)-1} \leq \log_2 m$. Observe that for $p_1, \ldots, p_k$ all the prime factors of m, then $2^k \leq p_1 \cdots p_k \leq m$, and thus $k \leq \log_2 m$. Hence,

$$\phi(m) = m \prod_{r=1}^{k} \left(1 - \frac{1}{p_r}\right) \geq m \prod_{r=2}^{\lfloor \log_2 m + 1 \rfloor} \left(1 - \frac{1}{r}\right) = \frac{m}{\lfloor \log_2 m + 1 \rfloor}.$$

Furthermore, as $m \geq 2 \cdot 3 \cdot 3 \cdot 5^{k-2}$, we have that $4^{k-2} < \frac{m}{6}$, thus $2^{k-1} < 2\sqrt{\frac{m}{6}} < \sqrt{m}$. Therefore, $\log_2 m \geq \phi(m) - 2^{k-1} \geq \frac{m}{\log_2(2m)} - \sqrt{m}$ leads to $m \leq 200$. Hence, $k \leq 4$, and the above inequality now becomes

$$7 \geq \phi(m) - 8,$$

which gives $\phi(m) \leq 15$ (so $\phi(m) \leq 14$). Therefore,

$$14 \geq \phi(m) \geq m\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$$

resulting in $m \leq 122$; thus $k \leq 3$. That being the case, $6 \geq \phi(m) - 4$ and this gives us $10 \geq \phi(m) \geq m(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})$, implying that $m \leq 37$. Now we find that $5 \geq \phi(m) - 4$, and so $\phi(m) \leq 9$ (thus $\phi(m) \leq 8$), which yields $8 \geq \phi(m) \geq m(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})$. Consequently, $m \leq 30$. We have $\phi(m) - 2^{k-1} > 0$, for $7 \leq m \leq 30$ and we can conclude, accordingly, that for each such m the inequality $m > c^{\phi(m)-2^{k-1}}$ gives a restriction on c. All cases may now be verified to conclude the validity of the theorem. □

The following example serves as an illustration of Zsigmondy's Theorem.

Example 2.4.2. We consider the sequence of integers of the form

$$w_n = 2^n - 1,$$

where $1 \leq n \in \mathbb{N}$. This generates the following sample of elements of the sequence:

$$1, 3, 7, 15, 31, 63, \cdots.$$

We note that $w_1 = 1, w_4 = 15 = 3 \cdot 5$ (and $3 \mid w_2$), $w_6 = 63 = 3^2 \cdot 7$. It is evident that no primitive divisors exist for 63.

What follows is the statement of the Primitive Divisor Theorem which is an extension of Zsigmondy's theorem:

Theorem 2.4.3. *If $n \notin \{1, 2, 3, 4, 6\}$ then w_n has a primitive divisor except when $((\alpha_1, \alpha_2), n)$ is of the form $\left(\pm\left(\frac{a_1+\sqrt{\Delta}}{2}, \frac{a_1-\sqrt{\Delta}}{2}\right), n\right)$*

Table 2.1: The triples

n	(a_1, Δ)
5	$(1,5), (1,-7), (2,-40), (1,-11), (1,-15), (12,-76), (12,-1364)$
7	$(1,-7), (1,-19)$
8	$(2,-24), (1,-7)$
10	$(2,-8), (5,-3)$
12	$(1,5)(1,-7)(1,-11)(2,-56)(1,-15)(1,-19)$
13	$(1,-7)$
18	$(1,-7)$
30	$(1,-7)$

As indicated, this theorem is an extension of Zsigmondy's theorem, see [19], and was rediscovered, independently, by Birkhoff and Vandiver more than a decade later in the instance when the roots of the characteristic polynomial are integers. In 1913, Carmichael proved it for the case when the roots are real, see [3]. Building on the previous work of Stewart and Schinzel, see [15] and [16], Bilu, Hanrot and Voutier settled the problem in the case where the roots are complex nonreal, see [1].

Chapter 3

The Proof of Carmichael's Theorem

3.1 Introduction

In 1913, Carmichael established that for α_1 and α_2 real and n not equal to 1, 2 and 6, the Lucas numbers $w_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2}$ have one or more primitive divisors excluding $n = 12$, $a_1 = 1$ and $a_2 = -1$ (for the characteristic polynomial

$$f(X) = X^2 - a_1X - a_2 = (X - \alpha_1)(X - \alpha_2)),$$

see [3]. Schinzel established that for the roots of f complex, their quotient is not a root of 1, and if n is sufficiently large, then the nth term in the companion Lucas sequence has a primitive divisor, see [15]. In 1976, it was proven by Stewart that if $n = 5$ or $n > 6$ then there are a finite number of Lucas sequences that do not exhibit a primitive divisor and that such sequences may be determined, see [16].

The aim of this chapter is to present an alternative method of proof to Theorem 2.4.3, for the case when the roots are real. As $\frac{\alpha_1}{\alpha_2}$ is not a root of unity, we may make the supposition that $|\alpha_1| > |\alpha_2|$. If need be, we may substitute (α_1, α_2) by $(-\alpha_1, -\alpha_2)$

(i.e.), replace $(w_n)_{n\geq 0}$ by the sequence with general term $(-1)^{n-1}w_n$, which alters the sign of certain of its terms but does not affect the prime factors. We suppose, then, that $\alpha_1 > 0$. In particular, $\alpha_1 > |\alpha_2|$. Hence, $w_n > 0$ for all n. For what follows, we refer the reader to [3], [13] and [18].

We appeal to Lemmas 2.3.6 and 2.3.7 and the following one which we now state:

Lemma 3.1.1 (see [13]). *If $p = 2$, $p \mid w_n$ and $p^c \mid \frac{w_{pn}}{w_n}$, then $c = 1$ if n is even and $p^c \leq 3\alpha_1^2$, otherwise.*

We now state (without proof) the precise version of Zsigmondy's Theorem due to Carmichael, see [18].

Theorem 3.1.2. *If α and β are real numbers and distinct roots of the polynomial $f(z) = z^2 - Lz + M$ for L and M nonzero integers and $n \neq 1, 2, 6$. Then $D_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ contains at least one primitive divisor except when $n = 12$, $L = 1$, and $M = -1$.*

We now put forth an alternative proof to Carmichael's version of Theorem 2.4.3.

Proof. We write

$$\frac{x^n - 1}{x - 1} = \prod_{\substack{j \mid n \\ j > 1}} \Phi_j(x).$$

Recall that $\Phi_m(x) \in \mathbb{Z}[x]$ represents the cyclotomic polynomial with roots the primitive roots of unity of order $m \geq 1$. A homogenisation yields

$$w_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} = \prod_{\substack{j \mid n \\ j > 1}} \Phi_j(\alpha_1, \alpha_2).$$

The cyclotomic polynomial with $j > 1$ satisfies the relation $\Phi_j(x) = x^{\phi(j)}\Phi_j(\frac{1}{x})$, i.e. it is reciprocal. The verification of this relies on the observation that if ρ is a primitive root of unity of order j, then ρ^{-1} is also one. By the Viete relations, the constant coefficient of $\Phi_j(x)$ is

$$(-1)^{\phi(j)}\exp\left(\frac{2\pi i}{j} \sum_{\substack{1 \leq k \leq j \\ \gcd(k,j)=1}} k\right) = (-1)^{\phi(j)} e^{\frac{2\pi i j \phi(j)}{2j}} = (-1)^{\phi(j)} e^{\pi i \phi(j)} = (-1)^{2\phi(j)} = 1,$$

where, for $j > 1$

$$\sum_{\substack{1 \le k < j \\ \gcd(k,j)=1}} k = \frac{j\phi(j)}{2},$$

holds which is a consequence of the fact that if $1 \le j < k$, then $\gcd(j,k) = 1 \iff \gcd(j-k,j) = 1$. As $\Phi_j(x)$ is reciprocal, $\Phi_j(\alpha_1, \alpha_2)$ is a symmetric expression in α_1 and α_2. $\Phi_j(\alpha_1, \alpha_2)$ is an algebraic integer and by Galois theory, it is a rational number and therefore an integer. Letting $\Phi_n(\alpha_1, \alpha_2) = CD$, for C, D positive integers with all prime factors p of C having $t_p < n$, while for all prime factors of D we have $t_p = n$, then $D = 1$ if w_n has no primitive divisor. If $p \mid C$, then $p \mid w_j$ for some $j < n$. Thus we have $p \mid \gcd(w_j, w_n) = w_{\gcd(j,n)}$ as $p \mid w_n$. We can therefore substitute $\gcd(j,n)$ for j and make the supposition that $j \mid n$. Due to the fact that $\Phi_j(x) \mid \frac{x^n-1}{x^j-1}$, we find that $\Phi_n(\alpha_1, \alpha_2) \mid \frac{w_n}{w_j}$. Hence, $p \mid \gcd(w_j, \frac{w_n}{w_j})$. We may assume that $p \mid \frac{n}{j}$ by Lemma 2.3.6. We now replace j by $\frac{n}{p}$ and suppose that $n = pj$. Thus, $\Phi_j(\alpha_1, \alpha_2) \mid \frac{w_{pj}}{w_j}$. By Lemma 2.3.7, we have $p \mid\mid \frac{w_{pj}}{w_p}$ for p odd and for $p = 2$ we have $2^c \mid \frac{w_{pj}}{w_j}$, then $2^c < 3\alpha_1^2$. In addition, $c = 1$ unless $2 \mid\mid n$, $t_2 = 3$ and $3 \mid n$. Hence, we arrive at

$$C = 2^c \prod_{\substack{p \mid C \\ p \neq 2}} p,$$

where all prime factors p of C are divisors of n. Since $2^c < 3\alpha_1^2$, we conclude immediately that $C < 1.5\alpha_1^2 n$. Thus, if $D = 1$, it emerges that

$$\Phi(\alpha_1, \alpha_2) < 1.5\alpha_1^2 n.$$

In the above inequality we may substitute $1.5\alpha_1^2$ by 1 unless $t_2 = 3$, $2 \mid\mid n$ and $3 \mid n$. On the other hand, clearly

$$\Phi_n(\alpha_1, \alpha_2) = \frac{\alpha_1^n - \alpha_2^n}{\prod_{p \mid n}(\alpha_1^{\frac{n}{p}} - \alpha_2^{\frac{n}{p}})} \frac{\prod_{\substack{p<q \\ pq \mid n}} \left(\alpha_1^{\frac{n}{pq}} - \alpha_2^{\frac{n}{pq}}\right)}{\prod_{\substack{p<q<s \\ pqs \mid n}} \left(\alpha_1^{\frac{n}{pqs}} - \alpha_2^{\frac{n}{pqs}}\right)} \cdots .$$

Also, $\alpha_1^j - \alpha_2^j < 2\alpha_1^j$ for all $j \ge 1$, and evidently $\alpha_1^j - \alpha_2^j \ge \alpha_1^{j-1}$ for all $j \ge 1$. The above inequality is clear for $\alpha_2 < 0$ and when j is odd. For $\alpha_2 > 0$, it is the case that

$$\alpha_1^j - \alpha_2^j = (\alpha_1 - \alpha_2)(\alpha_1^{j-1} + \ldots + \alpha_2^{j-1}) \ge \sqrt{\Delta}\alpha_1^{j-1} \ge \alpha_1^{j-1}.$$

We now consider the case when $\alpha_2 < 0$ and j is even. We have

$$\alpha_1^j - \alpha_2^j = \alpha_1^j - (-\alpha_2)^j = (\alpha_1 + \alpha_2)\left(\alpha_1^{j-1} + \alpha_1^{j-2}|\alpha_2| + \cdots + |\alpha_2^{j-1}|\right) \geq r_1\alpha_1^{j-1} \geq \alpha_1^{j-1}.$$

Letting $\omega(n) = k$ for the number of distinct prime factors of n and $p_1 < \cdots < p_k$, for such primes, we arrive at

$$\Phi_n(\alpha_1, \alpha_2) > \frac{1}{2^{2^{k-1}}}\alpha_1^{n-\sum_{i=1}^{k}\frac{n}{p_i}+\sum_{1\leq i<j\leq k}\frac{n}{p_ip_j}+\cdots+(-1)^{k-1}\frac{n}{p_1\cdots p_k}-2^{k-1}} = \frac{1}{2^{2^{k-1}}}\alpha_1^{\phi(n)-2^{k-1}}.$$

By considering the latter inequality in conjunction with

$$\Phi(\alpha_1, \alpha_2) < 1.5\alpha_1^2 n,$$

it now unfolds that

$$1.5 \cdot 2^{2^{k-1}} \cdot n > \alpha_1^{\phi(n)-2-2^{k-1}}.$$

We note that $\alpha_1 = \frac{(r_1+\sqrt{\Delta})}{2}$, $r_1 \geq 1$ and $\Delta \geq 1$. Therefore, for $r_1 \geq 3$, then $\alpha_1 \geq 2$. If $r_1 = 1$, then $\Delta = 1 + 4r_2 \geq 5$, which shows that $\alpha_1 \geq \frac{(1+\sqrt{5})}{2}$. If $r_1 = 2$, then $\Delta = r_1^2 + 4r_2 > 0$, which implies that $\Delta \geq 8$ and therefore $\alpha_1 \geq 1 + \sqrt{2}$. We note that since $p_i \geq i + 1$ for all $i = 1, 2, \ldots, k$, it comes to the fore that

$$\phi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) \geq n\prod_{i=1}^{k}\left(1 - \frac{1}{i+1}\right) = \frac{n}{k+1}.$$

Now we would like to establish the validity of $\sqrt{\frac{8n}{3}} \geq 2^k$ for all $n \geq 2$. However, we are cognisant of the fact that the latter inequality is equivalent to $4^{k-2} \leq \frac{n}{6}$, the truth of which has been ascertained in the proof of Zsigmondy's theorem.

By invoking

$$1.5 \cdot 2^{2^{k-1}} \cdot n > \alpha_1^{\phi(n)-2-2^{k-1}},$$

we have

$$\frac{1}{\log(\frac{(1+\sqrt{5})}{2})}\left(\log(1.5n) + \sqrt{\frac{2n}{3}}\log 2\right) > \frac{2n\log 2}{\log(\frac{32n}{3})} - \sqrt{\frac{2n}{3}} - 2.$$

This gives $n < 272$ and, hence, $k \leq 4$. By the inequality

$$1.5 \cdot 2^{2^{k-1}} \cdot n > \alpha_1^{\phi(n)-2-2^{k-1}},$$

we have that

$$\frac{\log 384n}{\log\left(\frac{(1+\sqrt{5})}{2}\right)} > \frac{n}{5} - 10,$$

which leads to $n \leq 170$ and, hence, $k \leq 3$. From the latter inequality, we deduce that

$$\frac{\log(24n)}{\log\left(\frac{(1+\sqrt{5})}{2}\right)} > \frac{n}{4} - 6,$$

which implies that $n \leq 90$. For $\phi(n) - 2 - 2^{k-1} \geq 12$, we have

$$2160 \geq 1.5 \cdot 2^{2^{3-1}} \cdot n \geq 1.5 \cdot 2^{2^{k-1}} \cdot n > \alpha_1^{12},$$

which yields $\alpha_1 < 2160^{\frac{1}{12}} < 2$. The unique pair (α_1, α_2) is $(\alpha_1, \alpha_2) = (\frac{(1+\sqrt{5})}{2}, \frac{(1-\sqrt{5})}{2})$ for which $w_n = F_n$ is the nth Fibonacci number. After establishing that F_n has a primitive divisor for all $n \leq 90$, with the exception of $n \in \{1, 2, 3, 4, 6, 12\}$, it is sufficient to assume that $\phi(n) - 2 - 2^{k-1} \leq 11$, which occurs for the small number values of $n \leq 60$. For each of the values of $n \leq 42$, with the exception of $n = 10, 12$, one may prove that

$$\alpha_1 < (1.5 \cdot 2^{2^{k-1}} \cdot n)^{\frac{1}{\phi(n)-2-2^{k-1}}}.$$

The upper bound for the expression on the right is less than 31 and therefore $r_1 \in [1, 62]$, $|r_2| < 961$, $n \leq 60$. By employing Mathematica, the proof is complete. Our argument does not hold for the case $n = 10, 12$, as for these values of n, we have $\phi(n) - 2 - 2^{k-1} = 0$. However, for none of these values can we have $t_2 = 3, 3 \mid n$ and $2 \mid\mid n$ which shows that for these two values of n the inequality $C \leq 1.5 \cdot \alpha_1^2 n$ can be superseded by the stronger inequality $C \leq n$. With this improved inequality and by employing the sequence of arguments above, we arrive at $2^{2^{k-1}} n > \alpha_1^{\phi(n)-2^{k-1}}$ instead of

$$1.5 \cdot 2^{2^{k-1}} \cdot n > \alpha_1^{\phi(n)-2-2^{k-1}}.$$

The new exponent is now $\phi(n) - 2^{k-1} = 2$ for $n = 10, 12$ and so the latter inequality gives us a bound for α_1. □

Chapter 4

Two applications of Carmichael's Theorem

4.1 Introduction

We commence this chapter by invoking Carmichael's Theorem to resolve a problem related to the largest prime factor of $x^2 - 1$ when x tends to infinity in the set of natural numbers. The resolution of this problem utilises, inter alia, the fact that the sequence which is formed by the quotient of the ith solution and the minimal solution to the Pell equation $x^2 - dy^2 = 1$, as encountered in Section 2.3.1, is a Lucas sequence.

In the second instance, Carmichael's Theorem is also appealed to when determining the largest solution $F_3F_4F_5F_6F_8F_{10}F_{12} = 11!$ of the Diophantine equation $F_{m_1}F_{m_2}\ldots F_{m_k} = n_1!\ldots n_s!$ with positive integers $3 \leq m_1 \leq \cdots \leq m_k$ and $2 \leq n_1 \leq n_2 \leq \cdots \leq n_s$, see [10]. For this chapter extensive use was made of the following: see [1], [3], [6], [9], [10] and [17].

4.2 Application 1

Proposition 4.2.1. *We let $P(n)$ denote the maximal prime factor of n. The largest solution of $P(x^2-1) \leq 29$ is*

$$36171409^2 - 1 = 2^5 \cdot 3 \cdot 5 \cdot 7^3 \cdot 11 \cdot 13^3 \cdot 17 \cdot 23 \cdot 29^2.$$

Proof. Let $x^2 - 1 = dy^2$, for d square-free. The only primes that can divide d are the elements of the set $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$. There are, therefore, only 1023 possible values of d. Suppose that $(x_1(d), y_1(d))$ is the minimal solution of the Pell equation, $x^2 - dy^2 = 1$, for each d and let $(x_j(d), y_j(d))$ be its j-th solution. Let $w_j = \frac{y_j(d)}{y_1(d)}$, and we note that this is a Lucas sequence. We invoke the Primitive Divisor Theorem and discern that if $j \geq 31$ then $y_j(d)$ has a prime factor $\geq j-1 \geq 30$. Therefore, for each of the 1023 values that d can assume, it is sufficient to generate the first 30 terms of the sequence $(x_j(d))_{j \geq 1}$ and recognise that all naturals x, such that $P(x^2-1) \leq 29$, are obtained in this manner. Computing with Mathematica shows that out of all these $1023 \cdot 30 = 30690$ possibilities, $x = 36171409$ is the largest solution to our problem. □

4.3 Application 2

Two definitions and a theorem are in order to state so as to illuminate certain aspects of the proof of Theorem 4.3.4 below. The latter theorem was proved by Luca and Stănică, see [10]; henceforth we follow their argument closely.

Definition 4.3.1 (see [1]). *A Lucas pair (α_1, α_2) such that w_n has no primitive divisors will be referred to as an **n-defective** Lucas pair.*

Note that for an integer $n > 3$ we put $P'(n) = P\left(\frac{n}{gcd(n,3)}\right)$. In other words,

$$P'(n) = \begin{cases} 2, & \text{if } n \text{ has the form } 2^k \cdot 3 \\ P(n), & \text{otherwise} \end{cases}$$

Theorem 4.3.2 (Cyclotomic Criterion, see [1]). *Let $n > 4$ be an integer distinct from 6 and 12. Then a Lucas pair (α_1, α_2) is n-defective if and only if*

$$\Phi_n(\alpha_1, \alpha_2) \in \{\pm 1, \pm P'(n)\}.$$

Also, a Lucas pair (α_1, α_2) is 12-defective if and only if

$$\Phi_{12}(\alpha_1, \alpha_2) \in \{\pm 1, \pm 2, \pm 3, \pm 6\}.$$

Definition 4.3.3 (see [6]). *For m an element of the natural numbers, we define the **index of entry** (or **entry point**) $t_m = t_m(u_n)$ in an integer linear recurrence u_n to be the smallest k an element of the natural numbers with $m \mid u_k$ if such an index k exists, and let $t_m = \infty$ otherwise.*

Theorem 4.3.4 (see [10]). *The largest solution of the Diophantine equation*

$$F_{m_1} F_{m_2} \dots F_{m_k} = n_1! \dots n_s! \tag{4.3.1}$$

with positive integers $3 \leq m_1 < \cdots < m_k$ and $2 \leq n_1 \leq n_2 \leq \cdots \leq n_s$ is

$$F_3 F_4 F_5 F_6 F_8 F_{10} F_{12} = 11!.$$

Note that in the statement of the theorem, indices m_i are exluded from assuming the values 1 and 2 as $F_1 = F_2 = 1$, and $n_j \geq 2$ since $0! = 1! = 1$. Also, the numbers n_j are not necessarily distinct for $j = 1, \dots, s$. On the other hand, the numbers m_i are distinct for $i = 1, \dots, k$. The restriction on the m_i is important for in its absence the above equation will have infinitely many solutions. By the largest solution in the hypothesis, it is meant that if $(m_1, \cdots, m_k)$ are distinctly different positive integers ≥ 3 such that $F_{m_1} \dots F_{m_k}$ is a product of factorials, then $\{m_1, \dots, m_k\} \subseteq \{3, 4, 5, 6, 8, 10, 12\}$.

Proof. Let $3 \leq m_1 < \cdots < m_k$ and $2 \leq n_1 \leq n_2 \leq \cdots \leq n_s$ be integers satisfying equation (4.3.1) in the statement of Theorem 4.3.4. Also let $N_1 = m_k$ and $N_2 = n_s$.

Upper bounds are sought on the N_i, for $i = 1, 2$. We recall that for n any non-negative integer, we have that equation (1.2.1.1) holds. Our starting point is the recollection of a classical argument which culminates in the proof of the Primitive Divisor Theorem. We have

$$F_n = \prod_{1 \le k < n} \left(\alpha_1 - e^{\frac{2\pi i k}{n}} \alpha_2 \right).$$

For the cyclotomic polynomial, we have

$$\Phi_n(\alpha_1, \alpha_2) = \prod_{\substack{1 \le k < n \\ \gcd(k,n)=1}} \left(\alpha_1 - e^{\frac{2\pi i k}{n}} \alpha_2 \right).$$

The inclusion-exclusion principle gives

$$\Phi_n(\alpha_1, \alpha_2) = \frac{\alpha_1^n - \alpha_2^n}{\prod_{p|n} \left(\alpha_1^{\frac{n}{p}} - \alpha_2^{\frac{n}{p}} \right)} \frac{\prod_{\substack{p<q \\ pq|n}} \left(\alpha_1^{\frac{n}{pq}} - \alpha_2^{\frac{n}{pq}} \right)}{\prod_{\substack{p<q<s \\ pqs|n}} \left(\alpha_1^{\frac{n}{pqs}} - \alpha_2^{\frac{n}{pqs}} \right)} \cdots . \tag{4.3.2}$$

In the proof of Carmichael's Theorem, we have established that $\alpha_1^j - \alpha_2^j \ge \alpha_1^{j-1}$. In addition, $\alpha_1^j - \alpha_2^j < 2\alpha_1^j < \alpha_1^{j+2}$ for every positive integer j. Combining the latter two inequalities with equation (4.3.2) yields

$$\Phi_n(\alpha_1, \alpha_2) \ge \alpha_1^{\left(n - \sum_{p|n} \frac{n}{p} + \sum_{\substack{p<q \\ pq|n}} \frac{n}{pq} - \cdots \right) - 3 \cdot 2^{\omega(n)-1}} = \alpha_1^{\phi(n) - 3 \cdot 2^{\omega(n)-1}}.$$

To establish an upper bound on N_1, it is sufficient to suppose that N_1 is a large number. So suppose $N_1 > 12$. By the cyclotomic criterion it follows that there is a representation $\Phi_n(\alpha_1, \alpha_2) = C_n D_n$ with positive integers C_n and D_n, where $C_n \le n$ and all the prime factors of D_n are congruent to $\pm 1 (\mathrm{mod}\ n)$. Hence,

$$D_n \ge \frac{1}{n} \cdot \alpha_1^{\phi(n) - 3 \cdot 2^{\omega(n)-1}}. \tag{4.3.3}$$

The following claim is made: There is an N_0 such that if $N_1 > N_0$ then one of the following applies:

(i) $N_2 > N_1^{\frac{6}{5}}$;

(ii) If t is the smallest number belonging to $\{1, \ldots, s\}$ such that $n_t \geq N_1 - 1$, then $s - t + 1 > N_1^{\frac{1}{5}}$.

The challenge now is to prove the preceding claim and to find an appropriate value for N_0. We assume the contrary, i.e. that N_1 and N_2 are such that the claim is negated. In this regard, let p be an arbitrary prime number congruent to $\pm 1 (\mathrm{mod}\, N_1)$ and which divides $\prod_{i=1}^{s} n_i!$. Obviously, $p \geq N_1 - 1$, hence $p \mid \prod_{i=t}^{s} n_i! \mid (N_2!)^{s-t+1}$. An upper bound for the exact order at which p divides $(N_2!)^{s-t+1}$ is now required. The order at which p divides $N_2!$ equates to

$$\lfloor N_2/p \rfloor + \lfloor N_2/p^2 \rfloor + \cdots < \frac{N_2}{p} + \frac{N_2}{p^2} + \cdots = \frac{N_2}{p-1} \leq \frac{N_1^{\frac{6}{5}}}{N_1 - 2} < N_1^{\frac{1}{5}} + 2, \quad (4.3.4)$$

where, in the above inequality, use was made of the fact that $N_1 > 12$ and that $N_2 \leq N_1^{\frac{6}{5}}$, which shows that for $p \geq N_1 - 1$ and $p^{\gamma_p} \mid\mid (N_2!)^{s-t+1}$, then

$$\gamma_p < \left(N_1^{\frac{1}{5}} + 2\right)(s - t + 1) \leq N_1^{\frac{1}{5}} \left(N_1^{\frac{1}{5}} + 2\right).$$

Thus,

$$\prod_{\substack{p^{\gamma_p} \mid\mid (N_2!)^{s-t+1} \\ p \equiv \pm 1 (\mathrm{mod}\, N_1)}} p^{\gamma_p} \leq N_2^{N_1^{\frac{1}{5}} \left(N_1^{\frac{1}{5}} + 2\right) \left(\pi\left(N_1^{\frac{6}{5}}, N_1, -1\right) + \pi\left(N_1^{\frac{6}{5}}, N_1, 1\right)\right)}.$$

Here, $\pi(y, k, j)$ denotes the number of primes $p \leq y$ which are congruent to $j (\mathrm{mod}\, k)$. As $\pi(N_1^{\frac{6}{5}}, N_1, \pm 1) \leq N_1^{\frac{1}{5}} + 1$, we find that

$$\prod_{\substack{p^{\gamma_p} \mid\mid (N_2!)^{s-t+1} \\ p \equiv \pm 1 (\mathrm{mod}\, N_1)}} p^{\gamma_p} \leq \exp\left(2N_1^{\frac{1}{5}} \left(N_1^{\frac{1}{5}} + 2\right) \left(N_1^{\frac{1}{5}} + 1\right) \log\left(N_1^{\frac{6}{5}}\right)\right). \quad (4.3.5)$$

Since D_{N_1} is a divisor of the number appearing on the left hand side of the preceding inequality, it emerges from equation (4.3.3) and equation (4.3.5) that

$$\frac{1}{N_1}\cdot\alpha_1^{\phi(N_1)-3\cdot 2^{\omega(N_1)-1}} \leq D_{N_1} \leq \prod_{\substack{p^{\gamma_p}\|(N_2!)^{s-t+1}\\ p\equiv\pm 1(\mathrm{mod}\, N_1)}} p^{\gamma_p} \leq \exp\left(\frac{12}{5}N_1^{\frac{1}{5}}\left(N_1^{\frac{1}{5}}+2\right)\left(N_1^{\frac{1}{5}}+1\right)\log N_1\right).$$

When introducing logarithms, the above inequality transforms into

$$\left(\phi(N_1)-3\cdot 2^{\omega(N_1)-1}\right)\log\alpha_1-\log N_1 \leq \frac{12}{5}N_1^{\frac{1}{5}}(N_1^{\frac{1}{5}}+2)(N_1^{\frac{1}{5}}+1)\log N_1. \quad (4.3.6)$$

We now demonstrate that we can select $N_0 = 5\cdot 10^7$. To this end, we assume that $N_1 > 5\cdot 10^7$. In this case, we show that $3\cdot 2^{\omega(N_1)-1} < \sqrt{N_1}$. This inequality holds if $\omega(N_1) \leq 12$ since

$$3\cdot 2^{\omega(N_1)-1} \leq 6\cdot 2^{10} < 7\cdot 10^3 < \sqrt{N_1}.$$

We now suppose that $\omega(N_1) \geq 13$ and let $p_1 < p_2 < \ldots < p_j$ be the prime factors of N_1. We observe here that $j = \omega(N_1)$. Thus, $\sqrt{N_1} \geq \prod_{i=1}^{j}\sqrt{p_i}$. Since $\sqrt{p_j} \geq \sqrt{41} > 6$, $\sqrt{p_{j-1}} \geq \sqrt{37} > 4$ and $\sqrt{p_i} > 2$ is true for $i = 3,\ldots,j-2$, we have that $\sqrt{N_1} > 2^{j-2-3+1}\cdot 4\cdot 6 = 3\cdot 2^{j-1} = 3\cdot 2^{\omega(N_1)-1}$, which is required. Hence, for inequality (4.3.6) valid for some $N_1 > 5\cdot 10^7$, then

$$\left(\phi(N_1)-\sqrt{N_1}\right)\log\alpha_1-\log N_1 \leq \frac{12}{5}N_1^{\frac{1}{5}}(N_1^{\frac{1}{5}}+2)(N_1^{\frac{1}{5}}+1)\log N_1. \quad (4.3.7)$$

Using [17, Lemma 4.1], we have that $\phi(N_1) > \frac{N_1}{\log N_1}$ holds for all $N_1 \geq 2\cdot 10^9$. Thus, inequality (4.3.7) yields

$$\left(\frac{N_1}{\log N_1}-\sqrt{N_1}\right)\log\alpha_1-\log N_1 \leq \frac{12}{5}N_1^{\frac{1}{5}}(N_1^{\frac{1}{5}}+2)(N_1^{\frac{1}{5}}+1)\log N_1. \quad (4.3.8)$$

By employing Mathematica it is verified that the largest solution of the above inequality is $< 1.6\cdot 10^9$, a contradiction. Thus, $N_1 < 2\cdot 10^9$. By using [17, Lemma 4.2], we know that in this range $\phi(N_1) > \frac{N_1}{6}$. Hence, inequality (4.3.7) has, as a consequence, the following:

$$\left(\frac{N_1}{6} - \sqrt{N_1}\right) \log \alpha_1 - \log N_1 \leq \frac{12}{5} N_1^{\frac{1}{5}} (N_1^{\frac{1}{5}} + 2)(N_1^{\frac{1}{5}} + 1) \log N_1. \tag{4.3.9}$$

Again, with the use of Mathematica, the largest solution N_1 of the latter inequality is $< 7 \cdot 10^6$, which shows that the claim is correct for $N_0 = 5 \cdot 10^7$.

Next, we demonstrate that $N_1 \leq N_0$. We assume the contrary, that is, that $N_1 > N_0$. The truth of either (i) or (ii) follows from our earlier claim. If (i) is true, then the exponent at which 2 appears on the right hand side of the equation (4.3.1) is

$$\geq \lfloor N_2/2 \rfloor + \lfloor N_2/4 \rfloor + \cdots \geq N_2 - \frac{\log(N_2 + 1)}{\log 2} > N_1^{\frac{6}{5}} - \frac{\log(N_1^{\frac{6}{5}} + 1)}{\log 2}, \tag{4.3.10}$$

whereas if (ii) is valid, then the exponent at which 2 appears on the right hand side of equation (4.3.1) is

$$\geq (s - t + 1)\left(\lfloor (N_1 - 1)/2 \rfloor + \lfloor (N_1 - 1)/4 \rfloor + \ldots\right) > N_1^{\frac{1}{5}} \left(N_1 - 1 - \frac{\log N_1}{\log 2}\right). \tag{4.3.11}$$

It can be easily verified that, in our range, the right hand side of inequality (4.3.11) is less than the right hand side of inequality (4.3.10). Hence, in both cases, the order at which 2 appears on the right hand side of equation (4.3.1) is

$$> N_1^{\frac{1}{5}} \left(N_1 - 1 - \frac{\log N_1}{\log 2}\right). \tag{4.3.12}$$

It is a well known fact that, with reference to [9], if j is a positive integer and $2^j \mid\mid F_n$ then 3 is a factor of n for n odd if $j = 1$, and $n = 2^{j-2} \cdot 3 \cdot m$, where m is relatively prime to 6 for $j \geq 3$. From this, we deduce the exponent that appears in F_n is

$$\leq 2 + \frac{\log(\frac{n}{3})}{2} = \frac{\log(\frac{4n}{3})}{\log 2}.$$

Due to the fact that

$$F_{m_1}F_{m_2}\ldots F_{m_k} \mid \prod_{n=1}^{N_1} F_n,$$

we can further deduce that the order at which 2 appears on the left hand side of equation (4.3.1) is not greater than

$$\frac{1}{\log 2}\sum_{n=1}^{N_1}\log\left(\frac{4n}{3}\right) \leq N_1\frac{\log\left(\frac{4N_1}{3}\right)}{\log 2}. \tag{4.3.13}$$

The comparison of inequality (4.3.12) and inequality (4.3.13) yields

$$N_1^{\frac{1}{5}}\left(N_1 - 1 - \frac{\log N_1}{\log 2}\right) < N_1\frac{\log\left(\frac{4N_1}{3}\right)}{\log 2}. \tag{4.3.14}$$

The largest solution to this inequality is such that $N_1 < 7\cdot 10^6$. This contradicts the fact that $N_1 \geq N_0$. Consequently, any solution of equation (4.3.1) has $N_1 \leq N_0$. We now demonstrate that $N_2 < 10^{14}$. From Stirling's Formula, we can conclude that

$$\prod_{n=1}^{N_1} F_n \geq F_{m_1}\ldots F_{m_k} \geq N_2! \geq \left(\frac{N_2}{e}\right)^{N_2}.$$

As the inequality $F_n < \alpha_1^n$ is true for all positive integers n, we have that

$$\left(\frac{N_2}{e}\right)^{N_2} < \alpha_1^{\sum_{i=1}^{N_1} i} = \alpha_1^{\frac{N_1(N_1+1)}{2}}.$$

When introducing logarithms and considering the fact that $N_1 \leq N_0 = 5\cdot 10^7$, we arrive at

$$N_2\log\left(\frac{N_2}{e}\right) < \frac{N_0\left(N_0+1\right)\log\alpha_1}{2},$$

which implies that $N_2 < K_1 = 10^{14}$. We now consider the remaining case for $N_2 \leq 10^{14}$. We first assume that $N_2 \geq K_2 = 1069$. Here, 1069 is a factor of the right hand side of equation (4.3.1). The index of entry of 1069 is 89, but F_{89} has a 16 digit prime factor, viz. 1665088321800481, which is greater than K_1. Hence, $N_2 < K_2$. We now assume that $N_2 \geq K_3 = 73$. In this instance, the right hand side of equation (4.3.1)

is a multiple of K_3. The index of entry of 73 is 37, however, F_{37} is a multiple of the prime 2221 which is greater than 1069, hence, $N_2 < K_3$. We further assume that $N_2 \geq K_4 = 37$. In this situation, 37 is a factor of the right hand side of equation (4.3.1) and the index of entry of 37 is 19, but F_{19} has a prime factor of 113 which is greater than K_3, therefore $N_2 < K_4$. As a result, the largest prime factor of the number appearing on either side of equation (4.3.1) is less than or equal to 31. The Primitive Divisor Theorem justifies the conclusion that F_{N_1} has a prime factor greater than or equal to $N_1 - 1$ if $N_1 \geq 13$. Hence, $N_1 \leq 32$. By employing Mathematica once more, we see that the only Fibonacci numbers, F_n, with the largest prime factor less than or equal to 31 are those corresponding to $n \in \mathcal{B} = \{3, 4, \ldots, 10, 12, 14, 18, 24\}$. However, as $m_i \in \{9, 14, 18, 24\}$ for some $i = 1, \ldots, k$, we have $N_2 \geq 19$. More specifically, 5^3 is a divisor of the right hand side of equation (4.3.1). If $5 \mid F_n$ for some $n \in \mathcal{B}$, then $n \in \{5, 10\}$ and $5^2 \nmid F_n$ in both instances. We may now conclude that $n_i \in \{3, 4, 5, 6, 8, 10, 12\}$ and the product of all the Fibonacci numbers whose indices are elements of this last set is 11!. □

Bibliography

[1] Yu. Bilu, G. Hanrot and P. M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte", *J. Reine. Angew. Math.* **539** (2001), 75-122.

[2] G. D. Birkhoff and H. S. Vandiver, "On the integral divisors of $a^n - b^n$", *Ann. Math.* **5**(2) (1904), 173-180.

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

[4] D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*, Springer, New York, 2005.

[5] J. De Koninck and F. Luca, *Analytic Number Theory : Exploring the Anatomy of Integers*, American Mathematical Society, Providence, 2012.

[6] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, American Mathematical Society, Providence, 2003.

[7] I. N. Hernstein, *Abstract Algebra*, Prentice-Hall, New Jersey, 1996.

[8] F.T. Howard, *Applications of Fibonacci Numbers, Volume 9*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2004.

[9] E. Jacobson, "Distribution of the Fibonacci numbers mod 2^k", *Fibonacci Quart.* 30 (1992), 211-215.

[10] F. Luca and P. Stănică, "$F_1F_2F_3F_4F_5F_6F_8F_{10}F_{12} = 11!$", *Port. Math.* **63** (2006), 252-260

[11] M. Mignotte and N. Tzanakis, "Arithmetical study of recurrence sequences", *Acta Arith.*, LVII(1991), 357-364.

[12] R. A. Mollin, *Advanced Number Theory with Applications*, Chapman and Hall CRC, Boca Raton, 2010.

[13] P. Ribenboim, *My Numbers, My Friends : Popular Lectures on Number Theory*, Springer-Verlag, New York, 2000.

[14] H. E. Rose, *A Course in Number Theory*, Oxford Science Publications, New York, 1994.

[15] A. Schinzel, "Primitive Divisors of the Expression $A^n - B^n$ in Algebraic Number Fields", *J. Reine Angew. Math.* 268(269) (1974), 27-33.

[16] C. L. Stewart, "Primitive Divisors of Lucas and Lehmer Sequences." In Transcendence Theory: Advances and Applications, *Ed. A. Baker & W. Masser,* New York: Academic Press,(1977), 79-92.

[17] M. Ward, "The intrinsic divisors of Lehmer numbers", *Ann. Math.* 62(2) (1955), 230-236.

[18] M. Yabuta, "A simple proof of Carmichael's Theorem on Primitive Divisors", *Fibonacci Quarterly* ***39*** (2001), 439-443.

[19] K. Zsigmondy, "Zur theorie der Potenzreste", *Monatsh. Math.* **3** (1892), 265-284.