Members of Lucas sequences whose Euler function is a power of 2

Faye Bernadette (bernadette@aims-senegal.org)
African Institute for Mathematical Sciences (AIMS)
Senegal

Supervised by: Florian Luca
Fundación Marcos Moshinsky, UNAM, Mexico
fluca@matmor.unam.mx
Co-supervised by: Tall Amadou
AIMS Senegal

15 June 2013
Submitted in Partial Fulfillment of a Masters II at AIMS
Abstract

The regular polygon with \( n \geq 3 \) sides can be constructed with the ruler and the compass if and only if \( \phi(n) \) is a power of 2. This is a celebrated theorem of Gauss. Florian Luca showed that \( 34 = F_9 \) is the largest Fibonacci number whose Euler function is a power of 2. The goal of this project is to extend this result to any Lucas sequence whose roots are quadratic units. More precisely, let \( (u_n)_{n \geq 0} \) be the sequence given by \( u_0 = 0; u_1 = 1 \) and \( u_{n+2} = ru_n + 1 + su_n \) for all \( n \geq 3 \). The goal of this project is to prove that \( \phi(|u_n|) = 2^m \) has only finitely many positive integer solutions \((m, n)\) provided that \( s = \pm 1 \).

It’s the main theorem of this master thesis. The result is due to Faye B, Luca F, Tall A and Damir T.M.

Declaration

I, the undersigned, hereby declare that the work contained in this essay is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

BERNADETTE FAYE, 26 June 2013
Contents

Abstract i

1 Introduction 1

Introduction 1

1.1 Number Theory ................................................. 1
1.2 History about Fibonacci and Lucas sequences ................. 2
1.3 Primality of Fibonacci Numbers ................................ 5
1.4 Gauss theory ..................................................... 7

2 Preliminary notions 9

2.1 Linearly Recurrent sequences ................................. 9
2.2 The Euler function .............................................. 16
2.3 Fermat Primes Numbers ........................................ 18
2.4 Primitive root of unity ......................................... 18
2.5 Pell Equation \(y^2 - dx^2 = \pm 1\) ................................ 19
2.6 Gauss theorem ................................................... 23

3 Members of Lucas sequences whose Euler function is a power of 2 25

3.1 Members of Lucas sequences whose Euler function is a power of 2 25
3.2 Introduction ...................................................... 25
3.3 Preliminary results .............................................. 26
3.4 Proof of Theorem 3.2.1 ......................................... 29
3.5 Applications To Pell equations \(X^2 - dY^2 = \pm 1\) ............ 33

4 Conclusion 36

5 Computation of the factorisation of \(u_p^a\) for all \(p^a \leq 144\) 37

5.1 Value of \(u_p^a\) for \(r = 3\) from 1 to 144 Using Java ............ 37

References 42

References 44
1. Introduction

Numbers have fascinated people in various parts of the world over many centuries. Many results have been found on these numbers and was helpful to build a new area of science which is Number theory. During these last year, the “Fabulous Fibonacci numbers” are studied in many fields and lot of their interesting properties have been found. In [9], Florian Luca worked on 'Equations involving arithmetic functions of Fibonacci and Lucas numbers', and found the Fibonacci numbers which can be constructed with ruler and compass.

1.1 Number Theory

Number theory is the study of the set of positive natural numbers $1, 2, 3, 4, 5, 6, 7, \ldots$, which are often called the set of natural numbers [17]. We will especially want to study the relationships between different sorts of numbers. Since ancient times, people have separated the natural numbers into a variety of different types: odd, even, composite, triangular, square, prime, Fibonacci, Lucas \ldots

The main goal of number theory is to discover interesting and unexpected relationships between different sorts of numbers and to prove that these relationships are True. Furthermore, number theory is partly experimental and partly theoretical. The experimental part normally comes first; it leads to questions and suggests ways to answer them. The theoretical part follows; in this part one tries to devise an argument that gives a conclusive answer to the questions [17]. In summary, there are the following steps:

1. Accumulate data, usually numerical, but sometimes more abstract in nature.
2. Examine the data and try to find patterns and relationships.
3. Formulate conjectures (i.e., guesses) that explain the patterns and relationships. These are frequently given by formulas.
4. Test your conjectures by collecting additional data and checking whether the new information fits your conjectures.
5. Devise an argument (i.e., a proof) that your conjectures are correct.

All five steps are important in number theory and in Mathematics. More generally, the scientific method always involves at least the first four steps. In mathematics one requires the further step of a proof, that is, a logical sequence of assertions, starting from known facts and ending at the desired statement.

Furthermore, number theory is one of the more fascinating topics in mathematics and one of the reason is that several number theory problems can be formulated in simple terms with no or very little background required to understand their statements. That is why so many scientists have worked on famous problems and conjectures in number theory.

Else, for Analytic Number Theory, The use of analysis (real or complex) plays a large role in solving some number theory problems, in particular to the problem of distribution of prime numbers. In 1896
Jacques Hadamard and Charles Jean de la Vallée Poussin, using complex analysis, independently, prove the Prime Number Theorem namely the fact that \( \pi(x) \) is asymptotic to \( x / \log(x) \) as \( x \) tends to infinity, where \( \pi(x) \) stands for the number of prime numbers not exceeding \( x \). We are going along this thesis to study some properties of arithmetic and number theory, one part of mathematics which Gauss called "The Queen of Sciences".

1.2 History about Fibonacci and Lucas sequences

*From Rabbits To Numbers:* The Fibonacci sequence defined as

\[
\begin{align*}
F_0 &= 0 \\
F_1 &= 1 \\
F_{n+2} &= F_{n+1} + F_n \quad \text{for } n \geq 0
\end{align*}
\]
It begins with the following numbers: $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...$

This sequence is characterized by the fact that each term of the sequence is the sum of the last two previous terms. This sequence is introduce by Leonard of Pisa (surname Fibonacci).

Leonard of Pisa was a great mathematician, and worked on geometric and arithmetic. Leonardo Pisano-or Leonardo of Pisa, Fibonacci I-his name as recorded in history, is derived from the Latin "filius Bonacci," or a son of Bonacci", but it may more likely derive from "de filiis Bonacci", Family fibonacci. During his lifetime, Fibonacci traveled extensively to Egypt, Syria, Greece, Sicily, and Provence, where he not only conducted business but also met with mathematicians to learn their ways of doing mathematics. Indeed, Fibonacci sometimes referred to himself as "Bigollo," which could mean good-for-nothing or, more positively, traveler. Fibonacci was a serious mathematician, who first learned mathematics in his youth in Bugia, a town on the Barbary Coast of Africa, which had been established by merchants from Pisa. He may have liked the double meaning. When he returned to Pisa around the turn of the century, Fibonacci began to write about calculation methods with the Indian numerals for commercial applications in his book, Liber Abaci. Among the mathematical problems Fibonacci poses in chapter 12 of Liber Abaci, there is one about the generation of rabbits. Although its statement is a bit cumbersome, its results have paved the way for a plethora of monumental ideas, which has resulted in his fame today. Now, The Fibonacci Association, started in 1963, is a tribute to the enduring contributions of the master. They focus on Fibonacci numbers and related mathematics, emphasizing new results, research proposals, challenging problems, and new proofs of old ideas. Through The Fibonacci Quarterly, their official publication, many new facts, applications, and relationships about them can be shared worldwide. According to its official Web site, http://www.mses.dal.ca/Fibonacci/, "The Fibonacci Quarterly is meant to serve as a focal point for interest in Fibonacci numbers and related questions, especially with respect to new results, research proposals, challenging problems, and innovative proofs of old ideas."

This sequence describe the yearly evolution of a population of rabbits with this following simple rules:

- a couple of young rabbits be adults
- an adult couple give a young couple (which does not died for each generation)

These numbers were not identified as anything special during the time Fibonacci wrote Liber Abaci. As a matter of fact, the famous German mathematician and astronomer Johannes Kepler (1571 – 1630) mentioned these numbers in a 1611 publication 14 when he wrote of the ratios: "as 5 is to 8, so is 8 to 13, so is 13 to 21 almost". Centuries passed and the numbers still went unnoticed. In the 1830s C. F. Schimper and A. Braun noticed that the numbers appeared as the number of spirals of bracts on a pine cone.

In the mid 1800s the Fibonacci numbers began to capture the fascination of mathematicians. They took on their current name ("Fibonacci, 15 numbers") from Francois-Edouard-Anatole Lucas (1842 – 1891), the French mathematician usually referred to as "Edouard Lucas," who later devised his own sequence by following the pattern set by Fibonacci.

Lucas numbers form a sequence of numbers much like the Fibonacci numbers and also closely related to the Fibonacci numbers.
Instead of starting with 1, 1, 2, 3, . . . , Lucas thought of beginning with 1, 3, 4, 7, 11.....

This Lucas sequence became a generalization of Fibonacci sequence.

The Fibonacci series is defined recursively. That is, in order to find each term of the series using the definition, you have to find all the terms that precede it. We can write this definition formally as

\[
F_{n+2} = F_{n+1} + F_n \quad \text{for all } n \geq 1
\]

Or

\[
F_n = F_{n-2} - F_{n-1}
\]

This makes finding the \(n\)th term very difficult for large values of \(n\), as you must find every term that comes before \(n\). However, there could be a way to find Fibonacci numbers without using the definition. If this were possible, one would be able to find the \(n\)th term of the series simply by plugging \(n\) into a mathematical formula.

At 1843, the French mathematician Jacques-Philippe Marie Binet (1786 – 1856) developed a formula for finding any Fibonacci number given its position in the sequence. That is, with Binet’s formula

\[
1.2.1 \text{ Theorem.} \\
F_n = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right)
\]

In fact, in this formula, we can find the \(n\)th Fibonacci number without having to list the previous \((n - 1)\) numbers. Further, Binet’s formula involves two very special numbers, \(\frac{1 + \sqrt{5}}{2}\) and \(\frac{1 - \sqrt{5}}{2}\).
Many interesting properties have been found on Fibonacci and Lucas sequences, and they are used to solve some Diophantine equations and also used in cryptography. Much work have been done also to found the prime number on Lucas and fibonacci sequence.

Further, in [14], we found that there is (curiously enough) a method for testing if a number is a member of the Fibonacci sequence. The test goes this way:

1.2.2 Theorem. A number \( n \) is a Fibonacci number if (and only if) \( 5n^2 + 4 \) or \( 5n^2 - 4 \) is a perfect square.

Also, the problem of determining all perfect powers in the Fibonacci sequence and in the Lucas sequence was a famous open problem for over 40 years, and has been resolved only recently [3].

1.2.3 Theorem. ([1]) The only perfect powers among the Fibonacci numbers are \( F_0 = 0, F_1 = F_2 = 1, F_6 = 8 \) and \( F_{12} = 144 \). For the Lucas numbers, the only perfect powers are \( L_1 = 1 \) and \( L_3 = 4 \). In [4], it is shown that, the traditional approach to Diophantine equations involving Fibonacci numbers combines clever tricks with various elementary identities connecting Fibonacci and Lucas numbers. Theorem 1 was proved by combining some of the deepest tools available in Number Theory: namely the modular approach (used in the proof of Fermat’s Last Theorem) and a refined version of Baker’s theory of linear forms in logarithms. It also required substantial computations performed using the computer packages PARI/GP and MAGMA. The total running time for the various computational parts of the proof of Theorem 1 was about a week.

1.3 Primality of Fibonacci Numbers

A prime number is natural number that can be divided only, without leaving any remainder, by 1 and itself. Prime numbers, especially the large ones, are interesting to scientists. Large prime numbers are used as keys in the codes that are used to send secret messages. Since these are not easy to find, the codes are difficult to break. When you try to decide if a larger number is prime, you really only need to find out if it is divisible by prime numbers that are less than it is [19].

Every time we buy something on the internet with our credit card, we use prime numbers to keep our personal information secure; Using RSA cryptography.

Conjecture: Any generalized Fibonacci sequence whose initial two terms are coprime contains an infinite number of prime numbers?

1.3.1 Theorem. \( \forall (n, k) \in \mathbb{Z}^2, F_n \mid F_{nk} \)

1.3.2 Proof. • The case where \( nk = 0 \) is trivial

• and the case \( k < 0 \) can be deduce from the case \( k > 0 \). We can suppose \( k > 0 \) and \( n \neq 0 \)

For \( \alpha = \frac{1+\sqrt{5}}{2} \) and \( \beta = \frac{1-\sqrt{5}}{2} \)

\[
\frac{F_{nk}}{F_n} = \frac{\alpha^{nk} - \beta^{nk}}{\alpha^n - \beta^n} = \sum_{j=0}^{k-1} \left( \alpha^{(k-1-j)} \beta^{nj} \right)
\]
\[
= (\alpha^{n(k-1)} + \beta^{n(k-1)}) + (\alpha^{n(k-2)} \beta^n + \beta^{n(k-1)} \alpha^n) + (\alpha^{n(k-2)} \beta^{2n} + \beta^{n(k-1)} \alpha^{2n}) + \ldots
\]

\[
= (\alpha^{n(k-1)} + \beta^{n(k-1)}) + (-1)^n (\alpha^{n(k-3)} + \beta^{n(k-3)}) + (\alpha^{n(k-5)} + \beta^{n(k-5)}) + \ldots
\]

\[
= L_{n(k-1)} + (-1)^n L_{n(k-3)} + L_{n(k-5)} + \cdots \in \mathbb{Z}
\]

It is unknown whether there are infinitely many prime Fibonacci numbers first. We know that \(F_n\) divide \(F_{kn}\) and so, if \(n > 4\) if \(F_n\) is prime, \(n\) is prime. But the reciprocity is False \((F_{19} = 4181 = 37 \times 113\) is a counter-example).

At 1999, H.Dubner and W.Keller prove in [5], extending their previous searches for prime Fibonacci and Lucas numbers, found all probable prime Fibonacci numbers \(F_n\) have been determined for \(6000 < n < 50000\) and all probable prime Lucas numbers \(L_n\) have been determined for \(1000 < n < 50000\). A rigorous proof of primality is given for \(F_{9311}\) and for numbers \(L_n\) with \(n = 1097, 1361, 4787, 4793, 5851, 7741, 10691, 14449,\) the prime \(L_{14449}\) having 3020 digits. Primitive parts \(F_n\) and \(L_n\) of composite numbers \(F_n\) and \(L_n\) have also been tested for probable primality. Actual primality has been established for many of them, including 22 with more than 1000 digits. In a Supplement to the paper, factorizations of numbers \(F_n\) and \(L_n\) are given for \(n > 1000\) as far as they have been completed, adding information to existing factor tables covering \(n \leq 1000\).

Up to April 2010, the largest known probable prime Fibonacci number is \(F_{1968721}\), which has 411439 decimal digits (ref: Lifchitz, Nov. 2009).

Furthermore, the famous problem of determining all perfect powers in the Fibonacci sequence \((F_n)_{n>0}\) and in the Lucas sequence \((L_n)_{n>0}\) has recently been resolved by Y.Bugeaud, M. Mignotte and S. Siksek in [3].

In 1998, Florian Luca have proved in [9], that the largest Fibonacci numbers whose Euler function is a power of 2, is obtained when \(n = \pm 9\), and the only corresponding Lucas numbers which verifying these properties are \(n = 0, \pm 1, \pm 2, \pm 3\).

At February, 2013, F. Luca and P.Stanica have proved some diophantine results about the Euler function of Pell numbers and their Pell-Lucas companion sequence. They prove the following statements:

**1.3.3 Theorem.** Let \((P_n)_{n \geq 0}\) and \((Q_n)_{n \geq 0}\) be the Pell sequence and his companion of general terms

\[
P_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad Q_n = \alpha^n + \beta^n
\]

where \(\alpha = 1 + \sqrt{2}\) and \(\beta = 1 - \sqrt{2}\).

The following statements holds:
• The only nonnegative integer solutions of the equation $\phi(P_n) = 2^m$ are 

$$(n, m) \in \{(1, 0); (2, 0); (3, 2); (4, 2); (8, 7)\}$$

If $n > 1; t > 1$, the only nonnegative integer solutions to $\phi(P_t^n) = 2^m$ are $(n, t, m) = (2, t, t-1), t \geq 2$.

• The only nonnegative integer solutions of the equation $\phi(Q_n) = 2^m$ are $(n, m) \in \{(1, 0); (2, 1); (4, 4)\}$.

If $n > 1; t > 1$, there are no nonnegative solution to $\phi(Q_t^n) = 2^m$.

• The only nonnegative integer solutions of the equation $\phi(P_t^n) = 2^m$ are $(n, t, m) \in \{(1, t, 0)\}$. If $t > 1$.

• The equation $\sigma(Q_t^n) = 2^m$ does not have nonnegative integer solutions $(n, t, m) t \geq 1$.

The above Diophantine equations with the numbers $P_n$ and $Q_n$ replaced by the Fibonacci and Lucas numbers $F_n$ and $L_n$ were studied in [9].

We extend the above results for all Lucas sequences define by the following recurrence relation:

$$
\begin{align*}
  u_0 &= 0 \\
  u_1 &= 1 \\
  u_{n+2} &= ru_{n+1} + su_n
\end{align*}
$$

where $s = \pm 1$ and $r$ a nonzero integer.

## 1.4 Gauss theory

Regarded as one of the greatest scientific geniuses of all time, Carl Friedrich Gauss (1777-1855) made influential contributions to the study of number theory and many other fields. It was generally believed that polygons with a prime number of sides greater than five could not be constructed with a ruler and compass, since the number of sides could not be factored.

### 1.4.1 Definition. A constructible polygon is a regular polygon that can be constructed with compass and straightedge.

Some regular polygons are constructible with compass and ruler; A natural question arise: is it possible to construct all regular $n$-gons with compass and straightedge? If not, which $n$-gons are constructible and which are not? Gauss proved the constructibility of the regular $17$-gon in 1796 [20]. He has developed later the theory of Gaussian periods in his Disquisitiones Arithmeticae, which allowed him to formulate a sufficient condition for the constructibility of regular polygons:

### 1.4.2 Theorem. A regular $n$-gon can be constructed with compass and straightedge if $n$ is the product of a power of 2 and any number of distinct Fermat primes.

Gauss claimed that this condition was also necessary, but without proof. A full proof of necessity was given by Pierre Wantzel in 1837 in [15]. The result is known as the Gauss Wantzel theorem.

In this thesis, we focus our research on Members of Lucas sequences whose Euler function is a power of 2.
We will start by a brief history on Fibonacci numbers and Lucas sequences, and the main results obtained on this sequences.

We start with chapter 1 by defining the preliminary results about the linear recurrences sequences, Fibonacci and Lucas sequences, the Euler function, and the Pell equation.

In chapter 2, we present the proof of our main theorem on Lucas sequences whose Euler function is a power of 2, which is to prove that $\phi(|u_n|) = 2^m$ has only finitely many positive integer solutions $(m; n)$ provided that $s = \pm 1$. We will compute some examples as on Pell numbers.

Finally, we will conclude by giving some perspectives on our future work, consisting to apply these results in Cryptography.
2. Preliminary notions

In this chapter, we will define all the mathematical tools that are need in the proof of our main theorem. In particular, we will enumerate some properties about linearly recurrence sequences [13], Lucas and Fibonacci sequences, the Euler φ function and Pell equations.

We shall reference some theorems to the multitude of results that had been proved over recent years.

2.1 Linearly Recurrent sequences

2.1.1 Definition. In general, a linear recurrence sequence \((X_n)_{n \geq 0}\) of order \(k\) is

\[
\begin{align*}
X_0 &= a \\
X_1 &= b \\
&\vdots \\
X_n &= a_0X_{n-1} + a_1X_{n-2} + \cdots + a_{k-1}X_{n-k} \quad (\forall) \quad n \geq k
\end{align*}
\]

for \(n \neq k\), where \(a_0, a_1, \ldots, a_{k-1}\) are constants. The value \(X_0, \ldots, X_{k-1}\) are the initial conditions.

2.1.2 Example. For \(k = 3\),

\[
\begin{align*}
X_0 &= X_1 = 1 \\
X_2 &= 2 \\
&\vdots \\
X_n &= X_{n-1} + 2X_{n-2} + 3X_{n-3}
\end{align*}
\]

is a linear recurrence sequence.

When \(k = 2\) the linear recurrence sequence is called a linear binary recurrence sequence.

Linear recurrence sequences of order 2 and 3 are called binary and ternary linear recurrence sequences respectively. For a linear recurrence sequence of order \(n\), the \(n\) initial values determine all others elements of the sequence.

2.1.3 Definition. (The Characteristical polynomial). The characteristic polynomial of a linear recurrence,

\[
c_ku_{n+k} + c_{k-1}u_{n-k-1} + \cdots + c_1u_{n+1} + c_0u_n = 0
\]

is defined to be the polynomial,

\[
c_kx^{n+k} + c_{k-1}x^{n-k-1} + \cdots + c_1x^{n+1} + c_0x^n = 0
\]

The simplest of all linear recurrence sequences are geometric progressions, which are defined by the rule
\[
\begin{aligned}
X_0 &= 1 \\
X_{n+1} &= \alpha X_n
\end{aligned}
\]

Such a sequence has the property that

\[\frac{X_{n+1}}{X_n} = \alpha\]

That is the ratio of successive terms is \(\alpha\).

### 2.1.4 Example.

For example, the characteristic polynomial of the recurrence

\[u_{n+2} + 9u_{n+1} - 4u_n = 0\]

is

\[x^2 + 9x - 4 = 0.\]

We let this polynomial have roots \(\alpha_1, \alpha_2, \ldots, \alpha_k\). The formula for this sequence depends on whether or not the roots \(\alpha_1, \alpha_2, \ldots, \alpha_k\) are distinct. The condition that these roots are distinct is that the\n
**Discriminant** \(\Delta\), is nonzero. For this example, we have the following distinct roots:

\[
\left\{ \frac{-3 + \sqrt{65}}{2}, \frac{-3 - \sqrt{65}}{2} \right\}
\]

where \(\Delta = 65\)

### 2.1.5 Theorem. (Zsigmondy’s theorem):

If \(a > b > 0\) are coprime integers, then for any natural number \(n > 1\) there is a prime number \(p\) (called a primitive prime divisor) that divides \(a^n - b^n\) and does not divide \(a^k - b^k\) for any positive integer \(k < n\), with the following exceptions:

- \(a = 2, b = 1, \text{ and } n = 6; \text{ or}\)
- \(a + b\) is a power of two, and \(n = 2\).

**Proof.** see [16]

From Zsigmondy’s theorem, we have the following definition.

### 2.1.6 Definition. (Primitive prime divisors).

Let \(q\) be prime; \(q\) is call a primitive if \(q \mid u_n\), if \(q \nmid u_d\)

\(\forall d \mid n \text{ and } q \nmid \Delta.\) So,

\[n = p^a, d \mid n, d < n \Rightarrow d \mid p^{a-1}\]

### 2.1.7 Corollary.

Let \((u_n)\) be a linear recurrence sequence such that \(u_n = 2^l \prod p_i^{\beta_i}\) with \(\beta_i = 1 \forall i\) Let \(p\)

be a odd prime number such that \(p \nmid \Delta.\) If

\[\frac{U_{p^a}}{U_{p^{a-1}}} = q_1 q_2 \ldots q_k\]

it follows that \(q_i\) is primitive for \(U_{p^a}\). Further, \((\forall) i, q_i \equiv 1 \mod p^a.\)
Proof. (Ref: Theorem of primes divisors).

Since \( p^{a-1} \mid p^a \), we have that \( u_{p^a-1} \mid u_{p^a} \). So \( \exists k \) such that

\[
\frac{u_{p^a}}{u_{p^a-1}} = \frac{u_{p^a-1} \cdot k}{u_{p^a-1}} = k
\]

\[\Rightarrow k = q_1 q_2 \ldots q_k\]

\[\Rightarrow q_1 \mid k \Rightarrow q_1 \mid u_{p^a} \tag{2.1.1}\]

Further \( q_1 \nmid u_{p^a-1} \). In fact if

\[q_1 \mid u_{p^a-1},\]

\[\Rightarrow q_1^2 \mid u_{p^a}\]

which is a contradiction because \( u_n \) is square free and \( q_1 \) is a primitive prime for \( u_{p^a} \).

Further we have that \( q \nmid \Delta \). So, from [1], we have that \((\forall) q_i \equiv \pm 1 \pmod{p^a}\).

\[\square\]

2.1.8 Definition. (Non-degeneracy). The linear recurrence sequence (3.4.1) is degenerate if it has a pair of distinct roots whose ratio is a primitive root of unity. Conversely, if \( \alpha_i \neq \alpha_j \) for all \( 1 \leq i < j \leq k \), it is non-degenerate.

Furthermore, the study of an arbitrary linear recurrence sequence can be reduced to that of non-degenerate linear recurrence sequences.

2.1.9 Fibonacci Sequences.

2.1.10 Definition. An example of a linear binary recurrence sequence is the Fibonacci sequence

\[
\begin{aligned}
F_0 &= 0 \\
F_1 &= 1 \\
F_{n+2} &= F_{n+1} + F_n & \text{for } n \geq 0
\end{aligned}
\]

Further, the polynomial \( f(x) = x^2 - x - 1 \) is the characteristic polynomial for \( F_n \).

The property that the successive term ratios are constant, is not shared by the Fibonacci numbers; however, one can speculate that the ratio of successive Fibonacci numbers tends to a limit. That is, does there exist a number \( \varphi \) such that:

\[
\lim_{n \to \infty} \frac{F_{n+1}}{F_n} = \varphi?
\]
Indeed, this limit exist and we can find it: In fact, if \( n \) is a very big integer, then

\[
\frac{F_{n+1}}{F_n} \approx \varphi, \quad \frac{F_n}{F_{n-1}} \approx \varphi,
\]

\[\Rightarrow\]

\[
F_{n+1} = F_n + F_{n-1} \Rightarrow \frac{F_{n+1}}{F_n} = 1 + \frac{F_{n-1}}{F_n}
\]

\[\Rightarrow \varphi \approx 1 + \frac{1}{\varphi}\]

In fact, we get equality here by letting \( n \) tend to infinity; so,

\[
\varphi^2 - \varphi - 1 = 0.
\]

The limit \( \varphi \) is thus either

\[
\frac{1 + \sqrt{5}}{2}, \quad \frac{1 - \sqrt{5}}{2}
\]

The fact that this second ratio is negative means that it cannot be our \( \varphi \), and so,

\[
\varphi = \frac{1 + \sqrt{5}}{2}
\]

**Binet’s Formula**

2.1.11 Definition. Binet’s Formula is an explicit formula used to find the \( n^{th} \) term of Fibonacci sequence.

Indeed

2.1.12 Theorem. If \( F_n \) is the \( n^{th} \) Fibonacci number,

\[
F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{1}{\sqrt{5}} ((\alpha)^n - (\beta)^n)
\]

Where \( \alpha \) and \( \beta \) are the roots of the Characteristic polynomial of Fibonacci.

Proof. 

- for \( n = 0, 1 \) it’s trivial

- Assume that

\[
F_k = \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{(1 + \sqrt{5}) - (1 - \sqrt{5})},
\]

\[
F_{k-1} = \frac{(1 + \sqrt{5})^{k-1} - (1 - \sqrt{5})^{k-1}}{(1 + \sqrt{5}) - (1 - \sqrt{5})},
\]

Show that \( F_{k+1} = F_k + F_{k-1} \).

We have that:
\[ F_{k+1} = \left( \frac{1 + \sqrt{5}}{2} \right)^k - \left( \frac{1 - \sqrt{5}}{2} \right)^k + \left( \frac{1 + \sqrt{5}}{2} \right)^{k-1} - \left( \frac{1 - \sqrt{5}}{2} \right)^{k-1} \]

For
\[ \alpha = \frac{1 + \sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{1 - \sqrt{5}}{2}, \]

we have that:

\[ F_{k+1} = \frac{\alpha^k - \beta^k}{\alpha - \beta} + \frac{\alpha^{k-1} - \beta^{k-1}}{\alpha - \beta} = \frac{\alpha^{k-1}(\alpha + 1) - \beta^{k-1}(\beta + 1)}{\alpha - \beta} \]

\[ F_{k+1} = \frac{\alpha^{k-1}\left(\frac{1 + \sqrt{5}}{2} + \frac{2}{2}\right) - \beta^{k-1}\left(\frac{1 - \sqrt{5}}{2} + \frac{2}{2}\right)}{\alpha - \beta} \]

\[ F_{k+1} = \frac{\alpha^{k-1}(6 + 2\sqrt{5}) - \beta^{k-1}(6 - 2\sqrt{5})}{\alpha - \beta} \]

\[ F_{k+1} = \frac{\alpha^{k-1}(1 + \sqrt{5})^2 - \beta^{k-1}(1 - \sqrt{5})^2}{\alpha - \beta} \]

\[ F_{k+1} = \frac{\alpha^{k+1} - \beta^{k+1}}{\alpha - \beta} \]

Then
\[ F_{k+1} = \frac{(1 + \sqrt{5})^{k+1} - (1 - \sqrt{5})^{k+1}}{(1 + \frac{\sqrt{5}}{2}) - (1 - \frac{\sqrt{5}}{2})} \]

\[ \square \]

In the case where, \( X_0 = 2, X_1 = 1 \) and \( X_{n+2} = X_{n+1} + X_n \), we get the Lucas Sequence \( (L_n) \) and:

2.1.13 Theorem.

\[ L_n = \alpha^n + \beta^n \]

Proof.  
- for \( n = 0, 1 \) the result is trivial
- we will use Binet’s formula to get the expression of \( L_n \) Since \( L_n = F_{n-1} + F_{n+1} \), then

\[ L_n = F_{n-1} + F_{n+1} = \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} + \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \]

\[ = \frac{1}{\alpha - \beta} [\alpha^n \left( \frac{1}{\alpha} + \alpha \right) - \beta^n \left( \frac{1}{\beta} + \beta \right)] \]

if we substitute
\[ \alpha = \frac{1 - \sqrt{5}}{2}, \]
\[ \frac{1}{\alpha} + \alpha = \sqrt{5} = \alpha - \beta, \]
\[ \frac{1}{\beta} + \beta = -\alpha + \beta, \]

And then, the formula for Lucas numbers is:
\[ L_n = \alpha^n + \beta^n. \]

The sequence can also be extended to negative index \( n \) by rewriting the recurrence by:
\[ F_{n-2} = F_n - F_{n-1} \]

which gives the sequence of "negafibonacci" numbers and justify some properties of the following lemma:

2.1.14 Lemma. 1. \( F_{-n} = (-1)^n F_n \) and \( L_{-n} = (-1)^n L_n \)

2. \( 2F_{m+n} = F_m L_n + L_n F_m \) and \( 2L_{m+n} = 5F_m F_n + L_m L_n \)

3. \( F_{2n} = F_n L_n \) and \( L_{2n} = L_n^2 + 2(-1)^{n+1} \)

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

5. Let \( p > 5 \) be a prime number. if \( (\frac{5}{p}) = 1 \) then \( p \mid F_{p-1} \). Otherwise \( p \mid F_{p+1} \). where \( (\frac{a}{b}) \) is the Legendre symbol of \( a \) over \( b \)

6. \( (F_n, F_m) = F_{(n,m)} \) for all positive integers \( m \) and \( n \), where \( (a,b) = gcd(a,b) \)

7. if \( m \mid n \) and \( \frac{n}{m} \) is odd, then \( L_m \mid L_n \)

8. Let \( p \) and \( n \) be a positive integer such that \( p \) is odd prime. Then \( (L_p, F_n) > 2 \) if and only if \( p \mid n \) and \( n/p \) is even.

Proof. : See [2], [1],[9]

2.1.15 Theorem. 1) The only solutions of the equation:
\[ \phi(|F_n|) = 2^m \]
are obtained for \( n = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8, \pm 9 \)

2) The only solutions of the equation:
\[ \phi(|L_n|) = 2^m \]
are obtained for \( n = \pm 1, \pm 2, \pm 3 \)

Proof. : See [9]
2.1.16 Lucas sequences. A Lucas sequence is a generalization of sequences like Fibonacci sequences and Lucas numbers.

2.1.17 Definition. The Lucas sequences $U_n(r, s)$ and $V_n(r, s)$ is a integer sequence that satisfy the recurrence sequence

$$U_{n+2} = rU_{n+1} + sU_n,$$

where $r$ and $s$ are fixed positive integers.

More generally, Lucas sequences $U_n(r, s)$ represent sequences of polynomial in $r$ and $s$ with integer coefficients.

Clearly, $u_n$ is an integer for all $n \geq 0$. Let $\alpha$ and $\beta$ denote the two roots of the equation

$$x^2 - rx - s = 0$$

It has a Discriminant $\Delta = r^2 + 4s \geq 0$ and then the roots are

$$\alpha = \frac{r + \sqrt{\Delta}}{2} \quad \text{and} \quad \beta = \frac{r - \sqrt{\Delta}}{2}$$

Thus

$$\alpha + \beta = r,$$

$$\alpha\beta = s,$$

$$\alpha - \beta = \sqrt{\Delta},$$

and,

$$U_n = aa^n + b\beta^n \text{ for all } n \geq 0.$$
2.1.18 Example. $U(1, -3)$:
\{0, 1, 1, 4, 7, 19, 40, 97, 217, 508, 1159, 2683, 6160, 14209, 32689, 75316, 173383, 399331, \ldots, \}

$V(1, -3)$:
\{2, 1, 7, 10, 31, 61, 154, 337, 799, 1810, 4207, 9637, 22258, 51169, 117943, 271450, 625279, \ldots, \}

2.1.19 Theorem. Let $(u_n)_{n \geq 0}$ be a linear recurrence sequence. Then we have the following results:

- $u_{2n} = u_n v_n$ where $v_n$ is the corresponding Lucas sequence
- $(u_m, u_n) = u_{(m,n)}$ for all positive integer $n, m$
- the integer $u_n$ and $u_m$ are relatively coprime when $n$ and $m$ are relatively coprime.
- If $p \mid n$, then $u_p \mid u_n$.

Proof. : see [1]

2.2 The Euler function

2.2.1 Definition. The Euler function $\phi(n)$ for a positive integer $n$ counts the number of positive integers $m \leq n$ which are coprime to $n$, that is:
\[\phi(n) = \# \{1 \leq m \leq n : (m, n) = 1 \}.\]

Let $\mathbb{Z}/n\mathbb{Z}$ be the set of congruence classes $a \mod n$. This set is also a ring and and its invertibles elements form a group whose cardinality is $\phi(n)$. Lagrange’s Theorem from group theory tells us that the order of every element in a finite group is a divisor of the order of the group. In this particular case, this theorem implies that
\[a^{\phi(n)} \equiv 1 \pmod{n}\]
holds for all integers $a$ coprime to $n$. The above relation is known as the Euler Theorem.

2.2.2 Elementary properties of the Euler function.

2.2.3 Theorem. (The fundamental theorem of arithmetic). The standard form of $n$ is unique; apart from rearrangement of factors, $n$ can be expressed as a product of primes in one way only.

In others words, for any integer $n > 1$, 
\[n = \prod_k p_i^{\alpha_k}\]

2.2.4 Theorem. The Euler function $\phi(n)$ is multiplicative, ie
\[\phi(mn) = \phi(n)\phi(m) \quad \text{for all} \quad (m, n) = 1\]
Proof. If \((m, m') = 1\), \(a'm + am'\) runs through a complete set \((\text{mod } m)m'\) when \(a\) and \(a'\) runs through a complete set \((\text{mod } m)\) and \((\text{mod } m')\) respectively. Also, using Chinese remainder theorem we get that:
\[
(a'm + am', mm') = 1 \equiv (a'm + am', m) = 1, (a'm + am', m') = 1 \\
\equiv (am', m) = 1, (a'm, m') = 1 \\
\equiv (a, m) = 1, (a', m') = 1
\]

Hence, the \(\phi(mm')\) number less than and prime to \(mm'\) are the least positive residues of the \(\phi(m)\phi(m')\) values of \(a'm + am'\) for which \(a\) is prime to \(m\) and \(a'\) to \(m'\) and therefore
\[
\phi(mm') = \phi(m)\phi(m')
\]

2.2.5 Theorem. If \(n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}\), where \(p_1, \ldots, p_k\) are distinct primes and \(\alpha_1, \ldots, \alpha_k\) are positive integers, then
\[
\phi(n) = \prod p_i^{\alpha_i-1}(p_i - 1) = p_1^{\alpha_1-1}(p_1 - 1) \cdots p_k^{\alpha_k-1}(p_k - 1),
\]
and,
\[
\sigma(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right),
\]
where \(\sigma\) is the sum of divisors of \(n\).

Proof. If \(n = p^\alpha\) is a prime power, then \(\{p, 2p, 3p, \ldots, (p^{\alpha-1})p\}\) are the only positive integer \(m \leq p^\alpha\) which are not coprime to \(p^\alpha\) and there are \(p^{\alpha-1}\) of them. Thus \(\phi(p^\alpha) = p^\alpha - p^{\alpha-1}\). Furthermore, the only divisors of \(p^\alpha\) are of the form \(p^\beta\) with some \(\beta \in \{0, 1, \ldots, \alpha\}\) so that,
\[
\sigma(p^\alpha) = 1 + p + \ldots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}
\]

Now the results for both the Euler function \(\phi\) and the sum of divisors function \(\sigma\) follow because both \(\phi\) and \(\sigma\) are multiplicative.

2.2.6 Example.
\[
\phi(68) = \phi(2^2.17) = (2^2-1)(2-1)(17-1) = 2.16 = 32
\]
\[
\sigma(68) = 2 + 17 = 20
\]

2.2.7 Theorem. (The Fermat-Euler Theorem). If \((a, n) = 1\) then,
\[
\phi^{a(n)} \equiv 1 \pmod{n}.
\]
Proof. Let \( a_1, a_2, \ldots, a_{\phi(n)} \) be all positive integers less than \( n \) which are coprime to \( n \). Since \( (a, n) = 1 \), then the set \( a_1, a_2, \ldots, a_{\phi(n)} \) contains residus which are congruent to one of the integers \( a_1, a_2, \ldots, a_{\phi(n)} \) in some order. Taking the product of these congruences, we get that:

\[
(aa_1)(aa_2)\ldots(aa_{\phi(n)}) \equiv a_1a_2\ldots a_{\phi(n)} \pmod{n}
\]

Hence

\[
a^{\phi(n)}(a_1, a_2, \ldots, a_{\phi(n)}) \equiv a_1, a_2, \ldots, a_{\phi(n)} \pmod{n}
\]

Since \( (a_1, a_2, \ldots, a_{\phi(n)}, n) = 1 \), we can divide both sides by \( a_1, a_2, \ldots, a_{\phi(n)} \) and we get the desired result.

The Euler function is one of the tools which are used to solve one of the famous problems of elementary geometry which is the construction of a regular polygon of \( n \) sides.

### 2.3 Fermat Primes Numbers

**2.3.1 Definition.** A fermat number is a positive integer of the form

\[
F_n = 2^{2^n} + 1
\]

where \( n \) is a nonnegative integer.

**2.3.2 Example.** The first seven Fermat numbers are

\[
3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, \ldots
\]

**2.3.3 Theorem.** If \( 2^n + 1 \) is an odd prime, and \( n > 0 \), then \( n \) must be a power of 2.

**Proof.** If \( n \) is not a power of 2, i.e. \( n = ab \) where \( 1 \leq a, b \leq n \) and \( b > 1 \) is odd, then

\[
(2^a + 1) \mid (2^{ob} + 1)
\]

thus

\[
(2^a + 1) \mid (2^n + 1)
\]

because \( 1 < 2^a + 1 < 2^n + 1 \) then \( 2^n + 1 \) is not a prime. So, \( n \) must be a power of 2.

In other words, every prime of the form \( 2^n + 1 \) is a Fermat number, and such primes are called Fermat primes. Some of the known Fermat primes are \( F_0, F_1, F_2, F_3, F_4 \).

### 2.4 Primitive root of unity

**2.4.1 Definition.** \( t \) is call a primitive root \( q \)-th root of unity if \( t^q = 1 \) but \( t^r \) is not 1 for all \( r < q \).
Section 2.5. Pell Equation \( y^2 - dx^2 = \pm 1 \)

Assume that \( t^q = 1 \) and that \( r \) is the least positive integer such that \( t^r = 1 \). Then \( q = rk + s \) where \( 0 \neq s < r \). Also
\[
t^s = t^{q-kr} = 1
\]
So that \( s = 0 \) and \( r \mid q \).

Using Moivre-Formula, we have that the algebraic equation,
\[
t^n - 1 = 0
\]
has the roots,
\[
\alpha_k = \cos \left( \frac{2\pi k}{n} \right) + i \sin \left( \frac{2\pi k}{n} \right)
\]
Let \( \alpha_k \) such that
\[
\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}
\]
are distinct, \( \alpha_k \) is said to be primitive \( n \)-th of root of unity. Then all the above numbers represent the primitive \( n \)-th root of unity. Then we have the following theorem

**2.4.2 Theorem.** A necessary and sufficient condition for \( \alpha_k \) to be a primitive \( n \)-th of root of unity is that the integer \( k \) be prime with \( n \).

*Proof.** See [12] \qed

Further, the number of primitive \( n \)-th root of unity is equal to the number of integers \( \leq n \) and prime to \( n \), and consequently equals to \( \phi(n) \)

**2.4.3 Theorem.** Any \( q \)-th root of unity is a primitive \( r \)-root for some divisors \( r \) of \( q \). And a necessary and sufficient condition that the root \( k \) should be a primitive is that \( k \) should be prime to \( q \).

*Proof.** See [12] \qed

### 2.5 Pell Equation \( y^2 - dx^2 = \pm 1 \)

**2.5.1 Definition.** (Diophantine Equation). A Diophantine equation is an indeterminate equation whose unknowns are only allowed to be integer.

**2.5.2 Example.** A simple example, take the equation
\[
x^2 + y^2 = z^2.
\]
where a solution \((x, y, z)\) is a triple of integer. Then we have the familiar solutions \((3, 4, 5), (5, 12, 13), (8, 15, 17)\).

Sometimes, a certain diophantine equation have no solution in integer like \( x^2 + y^2 = 3 \), and others has one or more trivial solutions. Many question about these diophantine equation are on those who are no-trivial solution. For example, the famous Fermat equation is:
\[
x^n + y^n = z^n.
\]
2.5.3 Definition. (Pell Equation). A Pell equation is a Diophantine equation of the form

\[ x^2 - dy^2 = 1 \]  

(2.5.1)

where \( d \) is a nonsquare positive integer.

2.5.4 Example. Consider the following equation

\[ x^2 - 7y^2 = 1. \]

A trivial solution of this equation is \((\pm 1, 0)\) and among his solutions we have \((\pm 8, \pm 3)\) and \((\pm 127, \pm 48)\).

It is named after John Pell because of an error in attribution by Euler. Euler was aware of the work of Lord Brouncker, the first European mathematician to find a general solution of the equation, but apparently confused Brouncker with Pell.

The Pell equation has a habit of appearing in a variety of settings, some quite unexpected. Consider the simple problem of finding integers that are both triangular and square. A triangular number simply counts the number of points in a grid in which the first row contains a single point and each subsequent row contains one more point than the previous. Thus, the triangular numbers are 1, 3, 6, 10, 15, \ldots and are given by the formula \( x(x + 1)/2 \). A problem can be to search those integers \( x \) such that \( x(x + 1)/2 = y^2 \) for some integer \( y \).

This give the following equation

\[ 4x^2 + 4x = 8y^2 \text{ where } d = 8 \]

2.5.5 Definition. Pell Numbers. The Pell Numbers are an infinite sequence of integer. The Pell numbers are defined by the following recurrence relation:

\[ P_n = \begin{cases} 0 & \text{if } n = 0; \\ 1 & \text{if } n = 1; \\ 2P_{n-1} + P_{n-2} & \text{otherwise}. \end{cases} \]

The first few terms of the sequence are 0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, \ldots

The Pell Lucas-numbers, may be calculated by means of a recurrence relation similar to that for the Fibonacci numbers.

2.5.6 Theorem. If \( d \) is a natural number which is not a perfect square, there are infinitely many pairs of natural number \((x, y)\) which satisfy the Diophantine equation

\[ x^2 - dy^2 = 1 \]

Proof. : See [12]

2.5.7 Theorem. If \( d \) is any natural number which is not a perfect square, they are infinite many pairs of natural numbers \((x, y)\) which satisfy the inequality,

\[ |x^2 - dy^2| < 1 + 2\sqrt{d} \]
Section 2.5. Pell Equation $y^2 - dx^2 = \pm 1$

For the proof of this theorem we need the following lemma

2.5.8 Lemma. The inequality, 
$$ |x/y - a| < \frac{1}{y^2} $$
where $a$ is a real irrational number, has an infinity of solutions in relatively prime integers $(x, y)$.

Proof. : See [12]

Proof. : the number $\sqrt{a}$ is irrational, and by the above Lemma, there are infinitely many pairs of positive integers $(x, y)$ such that
$$ |x/y - \sqrt{a}| < \frac{1}{y^2} $$
We have further
$$ |x/y + \sqrt{a}| = |x/y - \sqrt{a} + 2\sqrt{a}| < \frac{1}{y^2} + 2\sqrt{a} $$
thus
$$ |x^2 - dy^2| = |x - \sqrt{a}y||x - \sqrt{a}y| < \frac{1}{y^2} + 2\sqrt{a} < 1 + \sqrt{a} $$
then the equation has an infinitely of solutions $(x, y)$. □

2.5.9 Theorem. If $d$ is a natural number which is not a perfect square, the Diophantine equation (3.4.2) has infinitely many solutions $x + y\sqrt{d}$. All solution with positive $x$ and $y$ are obtained by the formula
$$ x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, $$
where $x_1 + y_1\sqrt{d}$ is the fundamental solution of 3.4.3, where $n$ runs through all natural numbers and where
$$ \begin{cases} x_n = x_1^n + \sum (n_{2k})x_1^{n-2k}y_1^{2k}d^k \\ y_n = \sum (n_{2k-1})x_1^{n-2k+1}y_1^{2k-1}d^{k-1} \end{cases} $$

Proof. : See[12] □

2.5.10 Remark. The equation
$$ a^2 - db^2 = -1 \tag{2.5.2} $$
is solvable only for certain values of $d$. A necessary condition for this equation in $(x, y)$ is obviously that all odd prime factors of $d$ be of the form $4n + 1$. Further, if $d$ is even, it can not be divisible by $4$.

2.5.11 Theorem. Let $d$ is a natural number which is not a perfect square. Suppose that the equation (3.4.5) is solvable and that $a_1 + b_1\sqrt{d}$ is it fundamental solution. Then the number,
$$ (x_1 + y_1\sqrt{d}) = (a_1^2 + b_1^2\sqrt{d})^2 = a_1^2 + db_1^2 + 2ab_1\sqrt{d} $$
is the fundamental solution of equation (3.4.3). Further, if we put,
$$ a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n, \tag{2.5.3} $$
with

\[
\begin{align*}
  a_n &= a_1^n + \sum \left( \frac{n}{2k} \right) a_1^{n-2k} b_1^{2k} d^k \\
  b_n &= \sum \left( \frac{n}{2k-1} \right) a_1^{n-2k+1} b_1^{2k-1} d^{k-1}
\end{align*}
\]

then the equation (3.4.7) gives:

- All the solution with positive \( a \) and \( b \) of equation (2.4) when \( n \) runs through all positive odd integers.

- All the solution with \( x = a_n \) and \( y = b_n \) of equation (2.3) when \( n \) runs through all positive even integers.

Proof. See [12] \qed

2.5.12 Example. For the following Pell equation:

\[ x^2 - 2y^2 = 1 \]

\((x_1, y_1) = (\pm 1, 0)\) is the trivial solution. Hence, if \((x_1, y_1)\) and \((x_2, y_2)\) are two solutions of the equation then

\((x_3, y_3) = (x_1, y_1) \cdot (x_2, y_2)\)

where

\[ x_3 = x_1 x_2 + 2y_1 y_2, \quad y_3 = x_1 y_2 + y_1 x_2, \]

is also a solution of the equation because the set of the solutions \((x, y)\) of the equation form an abelian group with this above multiplication law. Since \((3, 2)\) is the smallest non-trivial solution, then

- \((3, 2) \cdot (3, 2) = (9 + 8, 12) = (17, 12)\)

- \((3, 2)^3 = (99, 70)\)

are also solutions of the equation.

Thus, by a composition of the successive powers of \((3, 2)\) we can get infinitely many solution of the above equation.
2.6 Gauss theorem

2.6.1 Theorem. A regular \( n \)-gon is constructible with ruler and compass if and only if \( n = 2^k + 1 \) (\( k \) a power of 2) or if \( n = 2^l p_1 p_2 \ldots p_k \) where \( l \) is a non-negative integer, \( k \) is a positive integer, and each \( p_i \) is a (distinct) Fermat prime.

Thus a necessary condition for the possibility of the construction of a polygon of \( n \) sides by Euclid’s methods, when \( n \) is not prime, is that it must take the form

\[
2^m (2^{2m_1} + 1)(2^{2m_2} + 1) \ldots (2^{2m_k} + 1)
\]

where \( m_1, m_2, \ldots, m_k \) are all different.

From this result it is clear that the polygons of 9, 14, 18, 21, 22, 25, \ldots sides cannot be constructed in this way. Finally, we must show that this condition is also sufficient.

2.6.2 Theorem. The regular polygon with \( n \geq 3 \) sides can be constructed with the ruler and the compass if and only if \( \phi(n) \) is a power of 2.

Proof. : If

\[
\phi(n) = 2^m,
\]

then

\[
n = 2^l \prod p_i \quad \text{with} \quad p_i = 2^{m_1} + 1 \quad \text{and} \quad p_i < p_j \quad \text{for all} \quad i < j.
\]

In fact, by Fundamental Theorem of Arithmetic we have

\[
n = \prod p_i^{\beta_i}.
\]

It follows that

\[
\phi(n) = \phi\left( \prod (p_i^{\beta_i}) \right) = \prod (p_i^{\beta_i-1}(p_i - 1)) = 2^{m_1}.
\]
So,

\[ p_i^{\beta_i - 1} \mid 2^{m_1} \quad \text{and} \quad (p_i - 1) \mid 2^{m_1}. \]

Then

\[ \beta_i = 1 \quad \text{and} \quad p_i = 2^{2^m} + 1. \]

Then we can say that the only solutions will be those who will be equal to \( n = 2^l \prod p_i \) where all the \( p_i \) are Fermat Primes.

Hence, the above theorem has the following immediate corollary into Fibonacci and Lucas numbers.

**2.6.3 Corollary.**

1. The only regular polygons that can be constructed with the ruler and the compass and whose number of sides is a Fibonacci number are the ones with 3, 5, 8, and 34 sides, respectively.

2. The only regular polygons that can be constructed with the ruler and the compass and whose number of sides is a Lucas number are the ones with 3 and 4 sides, respectively.

*Proof.* See [9] \( \square \)

In summary, we have that in the Gauss theory, lot of the above functions and properties are important. And in this chapter, we have defined all the tools that we will need for the proof of the main theorem in the next chapter.
3. Members of Lucas sequences whose Euler function is a power of 2

3.1 Members of Lucas sequences whose Euler function is a power of 2

Here, we show that if \( u_0 = 0, \ u_1 = 1 \) and \( u_{n+2} = ru_{n+1} + su_n \) for all \( n \geq 0 \) is the Lucas sequence with \( s \in \{ \pm 1 \} \), then there are only finitely many effectively computable \( n \) such that \( \phi(\vert u_n \vert) \) is a power of 2, where \( \phi \) is the Euler function. We illustrate our general result by a few specific examples. This generalizes prior results of the Florian Luca and others which dealt with the above problem for the particular Lucas sequences of the Fibonacci and Pell numbers.

3.2 Introduction

Let \( \phi(m) \) be the Euler function of the positive integer \( m \). It is well-known that for \( m \geq 3 \), the regular polygon with \( m \) sides is constructible with the ruler and the compass if and only if \( \phi(m) \) is a power of 2. This happens exactly when \( m \) is the product of a power of 2 and a square free number all whose prime factors are Fermat primes; i.e., prime numbers of the form \( 2^{2^n} + 1 \) for some \( n \geq 0 \). For more information on Fermat numbers, see [7].

In [10], Luca found all the Fibonacci numbers whose Euler function is a power of 2. In [11], Luca and Stanica found all the Pell numbers whose Euler function is a power of 2. Here, we prove a more general result which contains the results of [10] and [11] as particular cases. Namely, we consider the Lucas sequence \( (u_n)_{n \geq 0} \), with \( u_0 = 0, \ u_1 = 1 \) and \( u_{n+2} = ru_{n+1} + su_n \) for all \( n \geq 0 \), where \( s \in \{ \pm 1 \} \) and \( r \neq 0 \) is an integer. Put \( \Delta = r^2 + 4s \) and assume that \( \Delta \neq 0 \), so, in particular, \( (r, s) \neq (\pm 2, -1) \). It is then well-known that if we put

\[
(\gamma, \delta) = \left( \frac{r + \sqrt{\Delta}}{2}, \frac{r - \sqrt{\Delta}}{2} \right),
\]

then the so-called Binet formula

\[
u_n = \frac{\gamma^n - \delta^n}{\gamma - \delta} \quad \text{holds for all} \quad n \geq 0.
\]

We assume that \( \gamma/\delta \) is not a root of 1, which happens if \( (r, s) \neq (\pm 1, -1) \). Observe that this condition implies that \( \Delta = r^2 + 4s > 0 \). So, \( \gamma \) and \( \delta \) are real. If \( r < 0 \), we may replace \( (r, s) \) by \( (-r, s) \), whose effect is that it replaces the pair \( (\gamma, \delta) \) by the pair \( (-\delta, -\gamma) \), so, in particular, \( u_n \) by \( (-1)^{n-1}u_n \). Such a transformation does not change \( \vert u_n \vert \). Thus, we may assume that \( r > 0 \). In this case, we have \( \gamma > 1 \) and \( \delta = -s\gamma^{-1} \in \{ -\gamma^{-1}, \gamma^{-1} \} \). Furthermore, \( u_n > 0 \) for all \( n \geq 1 \). In fact, we have \( u_{n+1} \geq u_n \) for all \( n \geq 0 \) with the inequality being strict for \( n \geq 2 \). This is clear if \( r = 1 \), because then \( s = 1 \) and so \( u_n = F_n \), the \( n \)th Fibonacci number, while if \( r \geq 2 \), then, by induction on \( n \geq 0 \), we have

\[
u_{n+2} \geq 2u_{n+1} - u_n = u_{n+1} + (u_{n+1} - u_n) > u_{n+1}.
\]

We have the following theorem.
3.2.1 Theorem. Assume \( s = \pm 1 \), \( r > 0 \) be an integer, \( (r, s) \neq (2, -1), (1, -1) \). Suppose \( n > 0 \) is such that \( \phi(u_n) \) is a power of 2. Then writing \( n = 2^a p_1^{\alpha_1} \cdots p_k^{\alpha_k} \), where \( 3 \leq p_1 < \cdots < p_k \) are distinct primes and \( a_0, a_1, \ldots, a_k \) are nonnegative integers, we have that \( a_0 \leq 4 \) and \( p_1^{\alpha_1} < 2(r^2 + 3)^2 \) for all \( i = 1, \ldots, k \).

3.2.2 Example. Consider the case when \( u_n = F_n \) is the Fibonacci sequence and assume that \( \phi(F_n) \) is a power of 2. We have \( r = 1 \), therefore \( p_i^{\alpha_i} < 32 \) for \( i = 1, \ldots, k \). Since the Euler functions of \( F_7, F_{11}, F_{13}, F_{17}, F_{19}, F_{23}, F_{25}, F_{27}, F_{29}, F_{31} \) are not powers of 2, it follows that \( p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) is a divisor of \( 3^2 \times 5 \). Finally, since the Euler function of \( F_3 \) is not a power of 2, it follows that \( n \) is a divisor of \( 2^2 \times 3^2 \times 5 \), and now a very quick calculation shows that \( n \in \{1, 2, 3, 4, 5, 6, 9\} \), which is the main result from [10].

3.2.3 Example. Consider the case when \( u_n = P_n \), the Pell sequence and assume that \( \phi(P_n) \) is a power of 2. Then \( r = 2 \), so \( p_i^{\alpha_i} < 98 \) for \( i = 1, \ldots, k \). A quick calculation shows that of all odd prime power values of \( p^a < 98 \), the Euler function of \( P_{p^a} \) is a power of 2 only for \( p^3 = 3 \). Further, the Euler function of \( P_{16} \) is not a power of 2, so \( n \) is a divisor of \( 2^3 \times 3 \). Computing the remaining values, we get that the only values for \( n \) are in \( \{1, 2, 3, 4, 8\} \), which is the main result in [11].

3.3 Preliminary results

For a nonzero integer \( m \) we write \( \nu_2(m) \) for the exponent of 2 in the factorization of \( m \). We let \( \{v_n\}_{n \geq 0} \) for the companion Lucas sequence of \( \{u_n\}_{n \geq 0} \) given by \( v_0 = 2, v_1 = r \) and \( v_{n+2} = rv_{n+1} + sv_n \). Its Binet formula is

\[
v_n = \gamma^n + \delta^n \quad \text{for all} \quad n \geq 0. \tag{3.3.1}
\]

We have the following results. Recall that \( s \in \{\pm 1\} \).

3.3.1 Lemma. We have the following relations:

i) If \( r \equiv 0 \pmod{2} \), then

\[
\nu_2(u_n) = \begin{cases} 
0 & \text{if } n \equiv 1 \pmod{2}, \\
\nu_2(v) + \nu_2(n) - 1 & \text{if } n \equiv 0 \pmod{2}, 
\end{cases}
\]

and

\[
\nu_2(v_n) = \begin{cases} 
\nu_2(v) & \text{if } n \equiv 1 \pmod{2}, \\
1 & \text{if } n \equiv 0 \pmod{2}. 
\end{cases}
\]

ii) If \( r \equiv 1 \pmod{2} \), then

\[
\nu_2(u_n) = \begin{cases} 
0 & \text{if } n \not\equiv 0 \pmod{3}, \\
\nu_2(v^2 + s) & \text{if } n \equiv 3 \pmod{6}, \\
\nu_2(v^2 + s) + \nu_2(v^2 + 3s) + \nu_2(n) - 1 & \text{if } n \equiv 0 \pmod{6}, 
\end{cases}
\]

and

\[
\nu_2(v_n) = \begin{cases} 
0 & \text{if } n \not\equiv 0 \pmod{3}, \\
\nu_2(v^2 + 3s) & \text{if } n \equiv 3 \pmod{6}, \\
1 & \text{if } n \equiv 0 \pmod{6}. 
\end{cases}
\]
Proof. i) Say $r$ is even. If $\{w_n\}_{n \geq 0}$ is any binary recurrent sequence of recurrence $w_{n+2} = rw_{n+1} + sw_n$, then $w_{n+2} \equiv w_n \pmod{2}$. In particular, $w_n$ has the same parity as $w_0$ or $w_1$ if $n$ is even or odd, respectively. Since $v_0 = 2$, $v_1 = r$ are even, it follows that $v_n$ is always even. If $n = 2k$ is even, then

$$v_n = \gamma^{2k} + \delta^{2k} = (\gamma^2 + \delta^2)^k = v_k^2 \pm 2$$

is congruent to 2 modulo 4 because $2 \mid v_k$. If $n = 2k + 1$, then

$$v_{2k+1} = (\gamma + \delta) \left( \frac{\gamma^{2k+1} + \delta^{2k+1}}{\gamma + \delta} \right) = rw_k \quad \text{where} \quad w_k = c(\gamma^2)^k + d(\delta^2)^k,$$

where $c = \gamma/r$, $d = \delta/r$. Thus, $\{w_k\}_{k \geq 0}$ is a binary recurrent sequence of roots $\gamma^2$, $\delta^2$, whose sum is $\gamma^2 + \delta^2 = v_2$ is even and whose product is $\gamma^2\delta^2 = 1$. By the remark at the beginning of the proof, $w_k$ has the same parity as $w_0$ or $w_1$ if $k$ is even and odd, respectively, and since $w_0 = 1$, $w_1 = \gamma^2 + \delta^2 - \gamma\delta = v_2 = 1$ is odd, it follows that $w_k$ is always odd. This shows that $v_2(v_{2k+1}) = v_2(r)$ and takes care of the parity of $v_n$. For $u_n$, since $v_0 = 0$, $v_1 = 1$, it follows that $u_n$ is even or odd according to whether $n$ is even or odd, respectively. If $n$ is even and we write $n = 2k\ell$ with $k \geq 1$ and $\ell$ odd, then

$$u_n = u_{2k\ell} = \gamma^{2k} - \delta^{2k} - \left( \frac{(\gamma^2)^{\ell} - (\delta^2)^{\ell}}{\gamma - \delta} \right) = v_1v_2\cdots v_{2k-1} \left( \frac{(\gamma^2)^{\ell} - (\delta^2)^{\ell}}{\gamma^{2k} - \delta^{2k}} \right).$$

Since $v_1 = r$, and $v_2$ is congruent to 2 modulo 4 for all $i = 1, \ldots, k - 1$, the part about $v_2(u_n)$ when $n$ is even follows provided that we show that the factor in the parenthesis above is odd. But this is $w_{k\ell}$, where now $\{w_n\}_{n \geq 0}$ is the Lucas sequence of roots $\gamma^2$ and $\delta^2$, the sum of which is $v_{2k}$ which is even and the product of which is $(\gamma\delta)^{2k} = 1$, and now the fact that $w_k$ is odd when $\ell$ is odd follows by the argument at the beginning of the proof, because $w_1 = 1$ is odd. This takes care of (i).

ii) Say $r$ is odd. Then $u_{n+2} \equiv u_{n+1} + u_n \pmod{2}$ and the same is true for $\{v_n\}_{n \geq 0}$. Since $v_0 \equiv u_0 \equiv 0 \pmod{2}$ and $v_1 \equiv u_1 \equiv 1 \pmod{2}$, it follows that both $u_n$ and $v_n$ have the same parity as $F_n$, the $n$th Fibonacci number, which is even if and only if $3 \mid n$. This takes care of ii) when $3 \nmid n$. Now take $n = 3k$. Then

$$u_n = \frac{\gamma^{3k} - \delta^{3k}}{\gamma - \delta} = \frac{\gamma^3 - \delta^3}{\gamma - \delta} \left( \frac{(\gamma^3)^k - (\delta^3)^k}{\gamma^3 - \delta^3} \right) = (r^2 + s)w_k,$$

where $\{w_n\}_{n \geq 0}$ is the Lucas sequence of roots $\gamma^3 + \delta^3$ the sum of which is $r(r^2 + 3s)$, which is even and for which $v_2(r(r^2 + 3s)) = v_2(r^2 + 3s)$ and the product of which is $(\gamma\delta)^3 = -s^3$. Similarly

$$v_n = (\gamma^3)^k + (\delta^3)^k$$

is the companion Lucas sequence of $\{w_n\}_{n \geq 0}$. Since this new Lucas sequence has the property that its sum of roots (namely, its corresponding “$r^\nu$”) is $r^2 + 3s$ which is even, the results from i) apply to $w_k$ and its companion and give ii).

\[ \square \]

3.3.2 Lemma. We have the following relations:

i) If $r \equiv 0 \pmod{2}$ and $k \geq 2$, then

$$\nu_2(v_{2k} - 2) = v_2(r^2 + 4s) + 2v_2(r) + 2k - 4.$$
ii) If \( r \equiv 1 \pmod{2} \) and \( k \geq 2 \), then
\[
v_{2^k} \equiv 7 \pmod{8}.
\]

**Proof.** For \( k \geq 2 \), we write
\[
v_{2^k} - 2 = \gamma^{2^k} + \delta^{2^k} - 2 = (\gamma^{2^{k-1}} - \delta^{2^{k-1}})^2 = \Delta u_{2^{k-1}}^2,
\]
where \( \Delta = r^2 + 4s = (\gamma - \delta)^2 \). Thus, if \( r \) is even, we get, by Lemma 3.3.1, that
\[
\nu_2(v_{2^k} - 2) = \nu_2(\Delta) + 2\nu_2(u_{2^{k-1}}) = \nu_2(r^2 + 4s) + 2\nu_2(r) + 2(k - 2).
\]
If \( r \) is odd, then \( \Delta = r^2 + 4s \equiv 5 \pmod{2} \) and \( u_{2^{k-1}} \) is odd, by Lemma 3.3.1, so that the right-hand side of formula (3.3.2) is congruent to 5 \pmod{8} , which yields \( v_{2^k} \equiv 7 \pmod{8} \). □

**3.3.3 Lemma.** Let \( a, b \) be nonnegative integers with \( a \equiv b \pmod{2} \). Then
\[
u_a - \nu_b = \begin{cases} u_{(a-b)/2}v_{(a+b)/2} & \text{if } s = 1 \text{ or } a \equiv b \pmod{4}, \\ u_{(a+b)/2}v_{(a-b)/2} & \text{if } s = -1 \text{ and } a \equiv b + 2 \pmod{4}. \end{cases}
\]

**Proof.** Straightforward verification using Binet's formulas (3.2.1) and (3.3.1).

If \( s = 1 = \gamma \delta \Rightarrow \gamma = \delta^{-1} \)
\[
u_{(a-b)/2}v_{(a+b)/2} = \frac{(\gamma(a-b)/2 - \delta(a-b)/2)}{(\gamma - \delta)}(\gamma(a+b)/2 - \delta(a+b)/2)
\]
\[
u_{(a-b)/2}v_{(a+b)/2} = \frac{\gamma^a + \gamma(a-b)/2 \delta(a+b)/2 - \gamma(a+b)/2 \delta(a-b)/2 - \delta^a}{\gamma - \delta} = \frac{\gamma^a - \delta^a - \gamma^b - \delta^b}{\gamma - \delta}
\]

Then,
\[
u_{(a-b)/2}v_{(a+b)/2} = \nu_a - \nu_b
\]

If \( s = -1 = \gamma \delta \Rightarrow \gamma = -\delta^{-1} \) and \( a \equiv b + 2 \pmod{4} \),
\[
u_{(a-b)/2}v_{(a+b)/2} = \frac{(\gamma(a-b)/2 - \delta(a-b)/2)}{(\gamma - \delta)}(\gamma(a+b)/2 - \delta(a+b)/2)
\]
\[
u_{(a-b)/2}v_{(a+b)/2} = \frac{\gamma^a + \gamma(a-b)/2 \delta(a+b)/2 - \gamma(a+b)/2 \delta(a-b)/2 - \delta^a}{\gamma - \delta} = \frac{\gamma^a - \delta^a - \gamma^b - \delta^b}{\gamma - \delta}
\]

Then,
\[
u_{(a-b)/2}v_{(a+b)/2} = \nu_a - \nu_b
\]

□
3.4 Proof of Theorem 3.2.1

We use the fact that if \( \phi(m) \) is a power of 2 and \( d \) is a divisor of \( m \), then \( \phi(d) \) is a power of 2 as well.

We assume that \( n > 1 \), \( \phi(u_n) \) is a power of 2 and \( p^a \| n \) and we want to bound \( p^a \). We proceed in various steps.

Case 1. \( p \) is odd and \( p \mid \Delta \).

It is well-known that \( p \mid u_n \).

In fact, if

\[
p \mid \Delta \Rightarrow p \mid u_n
\]

because

\[
\frac{\gamma^{p} - \delta^{p}}{\gamma - \delta} = \frac{(r+p\sqrt{\Delta})^p - (r-p\sqrt{\Delta})^p}{2p\Delta}
\]

\[
u_p = \frac{1}{2p}(pr^{p-1}\sqrt{\Delta} + \ldots) - (r^{p} - (\frac{p}{3})p^{3}\delta + \ldots + \Delta^{\frac{p-1}{2}})
\]

Then

\[
p \mid u_p \mid u_n \Rightarrow p \mid u_n
\]

Furthermore, if \( p^2 \mid n \), then \( p^2 \mid u_n \), because

\[
p^2 \mid u_p \mid u_n
\]

Since \( \phi(u_n) \) is a power of 2, it follows that it is not possible that \( p^2 \mid n \), therefore \( a \leq 1 \). Thus, in this case

\[
p^a \leq p \leq \Delta = r^2 + 4s < (r^2 + 3)^2.
\]

Case 2. \( p \geq 5 \) and \( p \nmid \Delta \).

We consider the number \( u_{p^a}/u_{p^{a-1}} \), which is a divisor of \( u_n \). Since it is also a divisor of \( u_{p^a} \) and \( p \geq 5 \), it follows, by Lemma 3.3.1, that \( u_{p^a}/u_{p^{a-1}} \) is an odd number larger than 1 because \( u_{m+1} > u_m \) for all \( m \geq 2 \). Since the Euler function of the odd number \( u_{p^a}/u_{p^{a-1}} > 1 \) is a power of 2, it can be written as

\[
\frac{u_{p^a}}{u_{p^{a-1}}} = q_1q_2\ldots q_t, \ \text{where} \ q_i = 2^{2^{n_i} + 1} \ \text{is prime for} \ 1 \leq i \leq t. \tag{3.4.1}
\]

We assume that \( n_1 < \cdots < n_t \). We look at the smallest prime factor \( q_1 \) of \( u_{p^a}/u_{p^{a-1}} \). Since \( p \nmid \Delta \), it follows that \( q_1 \) is primitive for \( u_{p^a} \). In particular, \( q_1 \equiv \pm 1 \pmod{p^a} \). If \( q_1 \equiv 1 \pmod{p^a} \), then, since \( q_1 = 2^{2^{n_1} + 1} \), it follows that \( 2^{2^{n_1} + 1} \equiv 1 \pmod{p^a} \). Thus, \( p \mid 2^{2^{n_1}} \), which is false. Hence, \( q_1 \equiv -1 \pmod{p^a} \), therefore

\[
2^{2^{n_1} + 1} = -1 + p^a\ell \ \text{for some integer} \ \ell. \tag{3.4.2}
\]

Since \( p \geq 5 \), it follows that \( n_1 \geq 2 \). Further, reducing the above relation modulo 4, we get that \( 2 \| \ell \). Thus, we have that

\[
p^a \leq \frac{2^{2^{n_1}} + 2}{\ell} \leq 2^{2^{n_1} - 1} + 1.
\]
Since the number $2^{2n_1-1} + 1$ is a multiple of 3 and $p \geq 5$, the above inequality implies that in fact

$$p^\alpha < 2^{2n_1-1}. \quad (3.4.3)$$

We now use a 2-adic argument to bound $n_1$ in terms of $p$. Namely, performing the multiplication on the right-hand-side of (3.4.1) above, we get that the right-hand-side of (3.4.1) is congruent to $1 + 2^{2n_1}$ (mod $2^{2n_1+1}$). Hence,

$$2^{2n_1} = \nu_2(u_{p^\alpha}/u_{p^{\alpha-1}} - 1) - \nu_2((u_{p^\alpha} - u_{p^{\alpha-1}})/u_{p^{\alpha-1}}). \quad (3.4.4)$$

Since $u_{p^\alpha-1}$ is odd, we get that

$$2^{2n_1} = \nu_2(u_{p^\alpha} - u_{p^{\alpha-1}}).$$

By Lemma 3.3.3, we get that

$$u_{p^\alpha} - u_{p^{\alpha-1}} = u_{p^{\alpha-1}(p+\varepsilon)/2}^{u_{p^{\alpha-1}(p-\varepsilon)/2}} \quad \text{for some} \quad \varepsilon \in \{\pm 1\}.$$ 

Since $p \geq 5$, exactly one of $p^{\alpha-1}(p \pm 1)/2$ is even and the other is odd, and exactly one is a multiple of 3 and the other is not. Invoking Lemma 3.3.1, we get that

$$2^{2n_1} = \nu_2(u_{p^\alpha} - u_{p^{\alpha-1}}) \leq \max\{\nu_2(u_{(p+\varepsilon)/2}), \nu_2((v_{(p-\varepsilon)/2}))\} + \nu_2(2). \quad (3.4.5)$$

The extra term $\nu_2(2)$ in fact appears only when $r$ is even and $(p + \varepsilon)/2$ is also even. Put $A = \nu_2(r) + \nu_2(r^2 + s) + \nu_2(r^2 + 3s)$. Note that $A \geq 1$. We distinguish two cases.

**Case 2.1** The maximum on the right-hand side of (3.4.5) is at most $A$.

In this case, $2^{2n_1-1} \leq 2^{A+\nu_2(r)-1}$. If $r$ is even, then $A = \nu_2(r)$, and therefore $2^{A+\nu_2(r)-1} \leq r^2/2$. If $r$ is odd, then $A = \nu_2(r^2 + s) + \nu_2(r^2 + 3s)$, and since $(r^2 + 3s) - (r^2 + s) = 2s = \pm 2$, it follows that $\min\{\nu_2(r^2 + s), \nu_2(r^2 + 3s)\} = 1$. Hence,

$$2^{A+\nu_2(r)-1} \leq \max\{r^2/2, r^2 + 3s, r^2 + s\} \leq r^2 + 3. \quad (3.4.6)$$

By inequality (3.4.3), we get that

$$p^{\alpha} < 2^{2n_1-1} \leq 2^{A+\nu_2(r)-1} \leq r^2 + 3. \quad (3.4.7)$$

**Case 2.2** The maximum on the right-hand side of (3.4.5) exceeds $A$.

A quick look at Lemma 3.3.1, shows that this case occurs only if the above maximum is at $\nu_2(u_{(p+\varepsilon)/2})$. Further, the condition $\nu_2(u_{(p+\varepsilon)/2}) > 2$ implies that $\nu_2((p + \varepsilon)/2) \geq 2$. Thus,

$$p + \varepsilon = 2^{\alpha+1}k \quad \text{holds with some odd number} \quad k \quad \text{and some} \quad \alpha \geq 2, \quad (3.4.8)$$

and relation (3.4.5) and Lemma 3.3.1 give

$$2^{n_1} = B + \alpha - 1 \quad (3.4.9)$$

for some $1 \leq B \leq A + \nu_2(r)$. In fact, it is easy to deduce that $B = A + \nu_2(r)$. In fact,
\[ \nu_2(u(\ell + \varepsilon)/2) = \begin{cases} \nu_2(r) + \alpha - 1 & r \text{ is even} \\ \nu_2(r^2 + s) + \nu_2(r^2 + 3s) + \alpha - 1 & r \text{ is odd} \end{cases} \]

Then,

- if \( r \) is even
  \[ 2^{n_1} = \nu_2(r) + \nu_2(r) + \alpha - 1 \]
- if \( r \) is odd
  \[ 2^{n_1} = 2\nu_2(r) + \nu_2(r^2 + s) + \nu_2(r^2 + 3s) + \alpha - 1 = A + \nu_2(r) + \alpha - 1 \]

Then \( B = A + \nu_2(r) \).

Thus, using also relation (3.4.2), we get

\[ -2 + \alpha \ell = 2^{2n_1} = 2B + \alpha - 1 = 2B - 1 \times 2^\alpha = 2B - 1 \left( \frac{p + \varepsilon}{2k} \right). \]  

We thus get that

\[ p(2k\ell p^{a-1} - 2B - 1) = 4k + \varepsilon 2B - 1. \]  

Assume first that the left-hand side of the formula (3.4.10) above is 0. Then \( 2k\ell p^{a-1} = 2B - 1 \). Since \( k \) is odd, \( 2\|\ell \), the only possibility is \( \ell = 2, a = 1, k = 1, B = 3 \). We then get \( 2^{n_1} + 1 = -1 + 2p \), therefore \( p = 2^{n_1} - 1, \) which is a multiple of 3, a contradiction. Thus, the left-hand side of equation (3.4.10) is nonzero. If \( k \geq 2B - 2 \), then \( 2k\ell \geq 4k \geq 2B \), so \( 2k\ell p^{a-1} - 2B - 1 \geq 2k \), so (3.4.10) gives

\[ p \leq \frac{4k + 2B - 1}{2k} = 2 + \frac{2B - 2}{k} \leq 3, \]

a contradiction. Thus, \( k < 2B - 2 \), so, by (3.4.10) again,

\[ p < 4 \cdot 2B - 2 + 2B - 1 \leq 3 \times 2B - 1 \leq 3 \times 2^{A + \nu_2(r) - 1} \leq 3(r^2 + 3), \]

where for the last inequality we have used inequality (3.4.6). Thus,

\[ 2^\alpha = \frac{p + \varepsilon}{2k} < 2(r^2 + 3), \]

therefore

\[ 2^{2n_1} = 2B + \alpha - 1 \leq 2^{A + \nu_2(r) - 1} 2^\alpha \leq (r^2 + 3) \times (2(r^2 + 3)) = 2(r^2 + 3)^2, \]

getting, by (3.4.3), that

\[ p^\alpha < 2^{2n_1 - 1} \leq (r^2 + 3)^2, \]

which is what we wanted to prove.

**Case 3.** \( p = 3 \) and \( p \nmid \Delta \).

Up to some minor particularities, this case is similar to the Case 2. We work again with \( u_3^\|=u_3^\alpha-1 \). If \( a = 1 \), then \( 3^\alpha = 3 < (r^2 + 3)^2 \), which is what we wanted. Suppose that \( a \geq 2 \). If \( r \) is even by Lemma
3.3.1, it follows that \( u_3^a \) is odd, so \( u_{3a}/u_{3a-1} \) is also odd. If \( r \) is odd, then \( \nu_2(u_{3a}) = \nu_2(r^2 + s) = \nu_2(u_{3a-1}) \), so \( u_{3a}/u_{3a-1} \) is also odd and it is larger than 1. We write again equation (3.4.1), as well as its conclusion (3.4.2). If \( n_1 = 1 \), we get \(-1 + 3^a \ell = 2^{21} + 1 = 5 \), showing that \( 3^a | 6 \), so \( a = 1 \), which is not the case we are treating. Thus, \( n_1 \geq 2 \), and (3.4.3) gives

\[
3^a < 2^{n_1-1}.
\] (3.4.11)

Equation (3.4.3) is

\[
2^{n_1} = \nu_2(u_{3a}/u_{3a-1} - 1) = \nu_2((u_{3a} - u_{3a-1})/u_{3a-1}).
\]

Since \( 3^a = 3^{a-1} + 2 \) (mod 4), we have, by Lemma 3.3.3,

\[
u_{3a} - u_{3a-1} = \begin{cases} u_{3a-1}v_{2x3a-1} & \text{if } s = 1 \\ u_{2x3a-1}v_{3a-1} & \text{if } s = -1. \end{cases}
\]

In particular,

\[
\frac{u_{3a} - u_{3a-1}}{u_{3a-1}} = v_{2x3a-1} \text{ or } v_{3a-1}^2
\]

according to whether \( s = 1 \) or \( s = -1 \). If \( r \) is even, we deduce, by Lemma 3.3.1, that \( 2^{n_1} \leq 2A \). If \( r \) is odd, then, again by Lemma 3.3.1, we deduce that \( 2^{n_1} \leq 2\nu_2(r^2 + 3s) \leq 2A - 2 \). Hence, at any rate, \( 2^{n_1} \leq 2A \), therefore

\[
2^{2n_1} \leq 2^{2A} = 4 \times (2^{A-1})^2 = 4(r^2 + 3)^2,
\]

where we used again inequality (3.4.6). By (3.4.11), we get

\[
3^a < 2^{n_1-1} \leq 2(r^2 + 3)^2,
\]

which is what we wanted.

Case 4. \( p = 2 \).

In this case, \( u_{2^a} | u_n \). Assume that \( a \geq 5 \). Then

\[
u_2(2a) = v_1 v_2 \cdots v_{2a-1}.
\]

Assume that \( r \) is odd. Lemma 3.3.2 shows that both \( v_4 \) and \( v_8 \) are congruent to 7 (mod 8). Since the only Fermat prime which is congruent to 3 modulo 4 is 3, and each one of \( v_4 \) and \( v_8 \) is a product of distinct Fermat primes, it follows easily that \( 3 | v_4 \) and \( 3 | v_8 \), so \( 9 | u_n \), a contradiction. So, in fact, \( a \leq 4 \) in this case.

Assume next that \( r \) is even and \( a \geq 5 \). Then \( v_4 v_8 v_{16} \) is a divisor of \( u_{2^a} \) and in particular its Euler function is a power of 2. By Lemma 3.3.2, we have

\[
\begin{align*}
\nu_2(v_4 - 2) &= \nu_2(r^2 + 4s) + 2\nu_2(r), \\
\nu_2(v_8 - 2) &= \nu_2(r^2 + 4s) + 2\nu_2(r) + 2, \\
\nu_2(v_{16} - 2) &= \nu_2(r^2 + 4s) + 2\nu_2(r) + 4.
\end{align*}
\]

Writing \( b = \nu_2(r^2 + 4s) + 2\nu_2(r) \), we get that

\[
\begin{align*}
v_4 &= 2q_1 \cdots q_t \text{ with } q_i = 2^{n_{ij}} + 1 \text{ where } n_1 < \cdots < n_t, \\
v_8 &= 2q_1' \cdots q_{t'} \text{ with } q_i' = 2^{n_{ij}'} + 1 \text{ where } n_1' < \cdots < n_{t'}', \\
v_{16} &= 2q_1'' \cdots q_{t''} \text{ with } q_i'' = 2^{n_{ij}''} + 1 \text{ where } n_1'' < \cdots < n_{t''}'.
\end{align*}
\]
and where furthermore $2^{n_1} = b$, $2^{n'_1} = b + 2$, $2^{n''_1} = b + 4$ and the sets

$$\{n_1, \ldots, n_t\}, \quad \{n'_1, \ldots, n'_t\} \quad \text{and} \quad \{n''_1, \ldots, n''_t\}$$

are mutually disjoint. Hence, $2^{n_1} + 2^{n''_1} = 2^{n'_1+1}(= 2b + 4)$, with distinct $n_1$, $n'_1$, $n''_1$, which is impossible by the uniqueness of the base 2 representation. This contradiction shows that in fact $a \leq 4$.

3.4.1 Examples. We are going to compute some examples for this Lucas sequences to show that everything works for the above theorem and to verify the bound for all $p^a \mid n$.

3.4.2 Example. In this case, let us take $r = 3$ and $s = -1$. Then

$$\begin{align*}
\{ \ &u_0 = 0 \\
&u_1 = 1 \\
&u_{n+2} = 3u_{n+1} - u_n
\end{align*}$$

From 5, we have the values of $u_n$ from $u_2$ to $u_{144}$. We have $r = 3$ therefore $p^a < (r^2 + 3)^2 = 144$. A quick calculation using PARI/GP, shows that of all odd prime power values of $p^a < 144$, the Euler function of $u_{p^a}$ is a power of two only for $p^a = 3$. Further, the Euler function of $u_4$ and $u_9$ are not a power of 2. Then $n$ is a divisor of $2 \times 3$. Computing the remaining values, we get that the only values are in $\{1, 2, 3, 6\}$. Then, this equation verifies the results of the theorem.

3.4.3 Example. In this case, let us take $r = 7$ and $s = 1$. Then

$$\begin{align*}
\{ \ &u_0 = 0 \\
&u_1 = 1 \\
&u_{n+2} = 7u_{n+1} + u_n
\end{align*}$$

We have the following results from $u_2$ to $u_{10}$:

\begin{align*}
\text{u(2)} &= 7.0 = 1 + 2.3 \\
\text{u(3)} &= 50.0 = 2.5^2 \\
\text{u(4)} &= 357.0 = 3.7.17 \\
\text{u(5)} &= 2549.0 = 2549 \text{ is prime} \\
\text{u(6)} &= 18200.0 = 2^3.5^2.7.13 \\
\text{u(7)} &= 129949.0 = 29.4481 \\
\text{u(8)} &= 927843.0 = 3.7.17.23.113 \\
\text{u(9)} &= 6624850.0 = 2^3.5^2.37.3581
\end{align*}

As we have seen above, a solution of the equation $\phi(u_n) = 2^m$ must be on the form $u_n = 2^l \prod p_k$. Then on the above list, they are no solution for this equation. Then this equation also verify the results of the theorem.

3.5 Applications To Pell equations $X^2 - dY^2 = \pm 1$

Consider the following Pell equation

$$X^2 - dY^2 = \pm 1$$
where \( d \) is a nonzero positive integer and a nonsquare. If \( d \) is a square or \( d < 0 \), it’s not hard to see that there are only the trivial solution \((\pm 1, 0)\).

Fermat was the first mathematician to conjecture that \( d > 0 \), and not a square, this equation have a infinitely many solutions. There always exist solution \((x, y)\) one positive integers.

Let \((x_1, y_1)\) be the minimal one. The all solutions are of the form

\[
\begin{align*}
  x_k + \sqrt{dy_k} &= (x_1 + \sqrt{dy_1})^k = \alpha^k, \\
  x_k - \sqrt{dy_k} &= (x_1 - \sqrt{dy_1})^k = \beta^k.
\end{align*}
\]

with \( \alpha = x_1 + \sqrt{dy_1} \) and \( \beta = x_1 - \sqrt{dy_1} \) we have,

\[
x_k = \frac{\alpha^k + \beta^k}{2},
\]

and,

\[
\frac{y_k}{y_1} = \frac{\alpha^k - \beta^k}{2\sqrt{dy_1}} = \frac{\alpha^k - \beta^k}{\alpha - \beta}.
\]

Further,

\[
\begin{align*}
  \alpha + \beta &= 2x_1 \\
  \alpha\beta &= 1
\end{align*}
\]

Then from this equation, we can generate the following linear recurrence sequence:

\[
\frac{y_k}{y_1} \Rightarrow u_{n+2} = ru_{n+1} + su_n,
\]

where

\[
\begin{align*}
  r &= 2x_1, \\
  s &= \pm 1.
\end{align*}
\]

**3.5.1 Example.** if \( d=3 \) we have that

\[
\begin{align*}
  \alpha &= 2 + \sqrt{3} \\
  \beta &= 2 - \sqrt{3}
\end{align*}
\]

Then,

\[
u_{n+2} = 4u_{n+1} - u_n.
\]

**3.5.2 Example.** Let us take the following Pell Equation:

\[
x^2 - 2y^2 = \pm 1
\]

\[
\begin{align*}
  \alpha &= 1 + \sqrt{2} \\
  \beta &= 1 - \sqrt{2}
\end{align*}
\]
And,

\[
\begin{cases}
    r = 2 \\
    s = -1
\end{cases}
\]

In this case, we have these following results:

\[
\begin{align*}
(1 + \sqrt{2})^2 &= 3 + 2\sqrt{2} \\
(1 + \sqrt{2})^3 &= 1 + 3\sqrt{2} + 6 + 2\sqrt{2} = 7 + 5\sqrt{2}
\end{align*}
\]

And \(49 - 2.25 = -1\)

We have seen that the above Diophantine equation has an infinitely many solutions and for a given equation, we can construct a linear recurrence sequence corresponding to this one.

However, let us replace \(x\) and \(y\) respectively by \(v_n\) and \(u_n\) the above Lucas Linear recurrence sequence. If we take \(u_n\) such that

\[
\phi(u_n) = 2^m
\]

According to the main theorem, we have a finitely many solutions for \((n, m)\). Then, If you put \(y = u_n\), we will have that the set,

\[
\#S = \{(x, y) : x^2 - dy^2 = \pm 1 \text{ and } y = u_n\} < \infty
\]

3.5.3 Example. Let us take the following Lucas sequence:

\[
\begin{cases}
    u_0 = 0 \\
    u_1 = 1 \\
    u_{n+2} = 3u_{n+1} - u_n
\end{cases}
\]

From 5, the principal solution of the main theorem are:

\[u_1 = 1, u_2 = 3, u_3 = 8 \text{ and } u_6 = 144.\]

If we apply this solutions on the Pell equation \(x^2 - 5y^2 = 1\) where \(y = \{u_1, u_2, u_3, u_6\}\) has the followings solutions:

\[(\sqrt{6}, 1), (4, 3), (\sqrt{41}, 8), (\sqrt{721}, 144)\]

And for \(x^2 - 5y^2 = -1\)

\[(2, 1), (\sqrt{144}, 3), (\sqrt{39}, 8), (\sqrt{719}, 144)\]
4. Conclusion

The work presented in this project, is the proof of the main Theorem on Lucas sequences with Gauss property, which can be construct as a regular polygon. We have also compute a few examples, like for the case of the Pell numbers, or when $u_n$ and $v_n$ are the $y$ and $x$ coordinates, respectively of some Pell equation $y^2 + dx^2 = \pm 1$ with a nonsquare positive integer $d$.

In summary, we have seen that one of the direct application of the main Theorem on our paper is to find finite solutions of these Pell equations.

Furthermore, in Cryptography both Fibonacci and Lucas sequences can be used for encryption/decryption purposes. The most important element of such a process is the creation of encryption/decryption key. The key can be a vector whose values are determined based on the result generated by the sequence. The future work would also involve seeking the possibility to find the opportunity to develop an asymmetric cryptosystem key based on this Lucas series for different values of $r$. 
5. Computation of the factorisation of $u_{p^a}$ for all $p^a \leq 144$

In this case, let us take $r = 3$ and $s = -1$. Then

\[
\begin{align*}
    u_0 &= 0 \\
    u_1 &= 1 \\
    u_{n+2} &= 4u_{n+1} - u_n
\end{align*}
\]

5.1 Value of $u_{p^a}$ for $r = 3$ from 1 to 144 Using Java

144
3.0
8.0
21.0
55.0
144.0
377.0
987.0
2584.0
6765.0
17711.0
46368.0
121393.0
317811.0
832040.0
2178309.0
5702887.0
1.4930352E7
3.9088169E7
1.0233415E8
2.6791429E8
7.0140873E8
1.8363119E9
4.8075269E9
1.2586269025E10
3.2951280099E10
8.6267571272E10
2.2585143371E11
5.9128672987E11
1.54800875592E12
4.052739537881E12
1.0610209857723E13
2.7777890035288E13
7.2723460248141E13
Section 5.1. Value of $u_p$ for $r = 3$ from 1 to 144 Using Java

<table>
<thead>
<tr>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.90392490709135E14</td>
</tr>
<tr>
<td>4.98454011879264E14</td>
</tr>
<tr>
<td>1.304969544928657E15</td>
</tr>
<tr>
<td>3.416454622906707E15</td>
</tr>
<tr>
<td>8.944394323791463E15</td>
</tr>
<tr>
<td>2.341672834846768E16</td>
</tr>
<tr>
<td>6.1305790721611576E16</td>
</tr>
<tr>
<td>1.6050064381636704E17</td>
</tr>
<tr>
<td>4.2019614072748954E17</td>
</tr>
<tr>
<td>1.100877783661015E18</td>
</tr>
<tr>
<td>2.880067194370815E18</td>
</tr>
<tr>
<td>7.5401138047463434E18</td>
</tr>
<tr>
<td>1.9740274219868217E19</td>
</tr>
<tr>
<td>5.16807085485831E19</td>
</tr>
<tr>
<td>1.353018523447067E20</td>
</tr>
<tr>
<td>3.542248481792618E20</td>
</tr>
<tr>
<td>9.273726921930787E20</td>
</tr>
<tr>
<td>2.4278932283999744E21</td>
</tr>
<tr>
<td>6.356306993006845E21</td>
</tr>
<tr>
<td>1.6641027750620561E22</td>
</tr>
<tr>
<td>4.356677625885484E22</td>
</tr>
<tr>
<td>1.1405930102594397E23</td>
</tr>
<tr>
<td>2.9861112681897712E23</td>
</tr>
<tr>
<td>7.817740794309874E23</td>
</tr>
<tr>
<td>2.046711111473985E24</td>
</tr>
<tr>
<td>5.358359254990967E24</td>
</tr>
<tr>
<td>1.4028366653498917E25</td>
</tr>
<tr>
<td>3.6726740705505786E25</td>
</tr>
<tr>
<td>9.615185546301844E25</td>
</tr>
<tr>
<td>2.5172882568354952E26</td>
</tr>
<tr>
<td>6.590346215876302E26</td>
</tr>
<tr>
<td>1.725375039079341E27</td>
</tr>
<tr>
<td>4.5170904956503927E27</td>
</tr>
<tr>
<td>1.1825896447871837E28</td>
</tr>
<tr>
<td>3.09605984765117E28</td>
</tr>
<tr>
<td>8.105590009602353E28</td>
</tr>
<tr>
<td>2.1220710144010545E29</td>
</tr>
<tr>
<td>5.555654042242929E29</td>
</tr>
<tr>
<td>1.4544891112327733E30</td>
</tr>
<tr>
<td>3.807901929474027E30</td>
</tr>
<tr>
<td>9.96921667189307E30</td>
</tr>
<tr>
<td>2.609974810209389E31</td>
</tr>
<tr>
<td>6.8330027629092365E31</td>
</tr>
<tr>
<td>1.788903347851832E32</td>
</tr>
<tr>
<td>4.683409767264573E32</td>
</tr>
<tr>
<td>1.2261325953941885E33</td>
</tr>
<tr>
<td>3.210056809456108E33</td>
</tr>
<tr>
<td>8.404037832974136E33</td>
</tr>
</tbody>
</table>
Section 5.1. Value of $u_{pe}$ for $r = 3$ from 1 to 144 Using Java

2.2002056689466297E34  
5.760213223542476E34  
1.508043001680798E35  
3.94810878149992E35  
1.036283234281895E36  
2.7060740824695694E36  
7.0845932398052E36  
1.854770768947199E37  
4.85582914443545E37  
1.271278974383438E38  
3.28251100870677E38  
8.713474505173687E38  
2.2812172414650384E39  
5.972304273877747E39  
1.5635695580168203E40  
4.0934782466626866E40  
1.071686518197124E41  
2.805711729925103E41  
7.345448671578187E41  
1.9230634284809458E42  
5.034645418285019E42  
1.3180872826374109E43  
3.4507973060837305E43  
9.03430463561378E43  
2.3652116600757614E44  
6.192204516665906E44  
1.6211401889921955E45  
4.2442001153099996E45  
1.111460156937791E46  
2.9090180355503376E46  
7.615908090957234E46  
1.9938706237321363E47  
5.220021062100686E47  
1.366619256256992E48  
3.57785662560907E48  
9.36694773142573E48  
2.4522987531716283E49  
6.420201486372312E49  
1.6808305705945311E50  
4.400471563146362E50  
1.1520584118844556E51  
3.0161280793387305E51  
7.896325826131737E51  
2.0672849399056482E52  
5.41222237103771E52  
1.4169381771405666E53  
3.7095923077113225E53  
9.711838745993401E53
Section 5.1. Value of $u_p^a$ for $r = 3$ from 1 to 144 Using Java

2.542592393026888E54
6.656593004481324E54
1.7427187520417084E55
4.5624969256769924E55
1.194772024989268E56
3.1271819149290812E56
8.18706854228317E56
2.143402371193587E57
5.6115002593519268E57
1.4691084068622E58
3.846179461234666E58
1.006942864768181E59
2.636210646929077E59
6.901689069310305E59

In fact, as we have seen, a solution of the equation $\phi(u_n) = 2^m$ must be on the form $u_n = 2^l \prod p_k$, where $p_k$ are fermat primes. Then on the above list, the only solutions are $u_2 = 3, u_3 = 8$ and $u_6 = 144$.

Using the function `Factor` in PARI/GP, we get the following values of the factorisation of $u_p^a$ for all odd prime power values with $p^a \leq 144$.

(14:47) gp > factor(55)
55 = 5.11
377 = 13.29
17711 = 89.199
121393 = 233.512
5702887 = 1597.3571
6580091406622738 = 2.43.173.1759.251432569
635630693006845 = 5.7.36683.4950761149
2046711111473995 = 3.5.11.1103.11245974403
1402836653498917 = 44262059.316938863
45170904956503927 = 311.1302121.111544217
21220710144010545 = 3.5.7.419.1181.58345673
145448491112327733 = 791003. 18387908911
4683409767264573 = 3^5.1927329122331
22002056689466297 = 61.360689453925677
708459392398052 = 2^2.181.593.607.2718523
1071686518197124 = 2^2.10277459.26068859
7345448671578187 = 67.10963562262361
503464518285019 = 37.487.1033.270481697
23652116600757614 = 2.178621.250037.264791
16211401889921955 = 3^2.5.19.106721.177666101
7615908090957234 = 2.3.59.401.53650535321
54122222237103771 = 991.5461374608581
2542592393026888 = 2^3.103.541.5703642107
8187068542288317 = 3.11.31.2789.6421.446891
5611500259351929 = 3^2.623500028816881
623500028818000 = 2^4.5^3.311750014409
Acknowledgements

Firstly, I thank God, Father of our Lord Jesus Christ for His infinite love and protection.

A special acknowledgement is due to my supervisor Professor Florian Luca, for his enthusiasm and patience throughout this essay, for his patient help and advices.

I would also like to thank Dr. Amadou Tall, first for the sake of mathematics that he give to me, for his participation in my training as he taught me ”in life, looking for two things: God and the knowledge”, and for his corrections and suggestions.

Big thanks to my team mate Damir Taoufiq, more than a friend who is now my co-author.

Special thanks to Tutors, all the staff of AIMS-Senegal and all those who supported me up to now, with their love, friendship, teachings, advices, encouragement, help, criticism, and patience.

Thanks to all my family, my dear mother, my dad, brothers and sisters, for their encouragement and support at all times.

God bless you!
References


[12] Trygve Nagell "Introduction to number theory" .-Stockholm, Almqvist and Wiksell, [ (1951) ]

[13] Notes on Linear Recurrence Sequences April 8, 2005


[21] www.google.sn (fibonacci:generation of rabbits,images)