# ON THE DIOPHANTINE EQUATION: JEŚMANOWICZ CONJECTURE AND SELECTED SPECIAL CASES

**ABDULRAHMAN HAMED AHMED BALFAQIH**

**UNIVERSITI SAINS MALAYSIA**

**2020**

# ON THE DIOPHANTINE EQUATION: JEŚMANOWICZ CONJECTURE AND SELECTED SPECIAL CASES

**by**

**ABDULRAHMAN HAMED AHMED BALFAQIH**

**Thesis submitted in fulfilment of the requirements**
**for the degree of**
**Doctor of Philosophy**

**November 2020**

# ACKNOWLEDGEMENT

First and foremost, I thank Allah the Almighty for giving me the blessings and strength to do this work. I would like also to express my sincere gratitude to my supervisor, Professor Dr. Hailiza Kamarulhaili for her guidance, advice, assistance, wide insights and unremitting support in helping me to complete this study. I was honored to have her as my supervisor. My gratitude extends to the staff at School of Mathematical Sciences for being the most dedicated people that I have ever met.

Special thanks go to my family, especially my father, May Allah have mercy on him, whose life and guidance was the light through which I managed to overcome all the hardships of life. I would like also to thank my mother for her continuous prayers and support. She is the person whom I can never thank.In addition I would like to thank my wife with my son Ahmed for their encouragement and continuous assistance.

My gratitude goes to Hadramout Establishment for their financial, intellectual, and emotional support. Without them, My academic journey would never commence.

Every member in Seiyun University and Hadramout University, also deserves my sincerest thanks. Their assistance has meant more to me than I could ever express.

Abdulrahman Hamed Ahmed Balfaqih

2020

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# LIST OF ABBREVIATIONS

**FMID** Fermat's Method of Infinite Descent

**BHV** Bilu, Hanrot and Voutier

**min** Minimum

**max** Maximum

# LIST OF SYMBOLS

| | |
|---|---|
| $\mathbb{N}$ | The set of natural numbers |
| $\mathbb{Z}$ | The set of integers |
| $\mathbb{Z}^*$ | The set of non-zero integers |
| $\mathbb{Z}^n$ | The set of $n$-tuple of integers |
| $\mathbb{R}$ | The set of real numbers |
| $f(x) \ll g(x)$ | If $f(x), g(x) \geq 0$, then there exists a constant $c$, such that $\lvert f(x)\rvert < c\,g(x)$ for sufficiently large values of $x$ |
| $f(x) \gg g(x)$ | If $f(x), g(x) \geq 0$, then there exists a constant $c$, such that $\lvert g(x)\rvert < c\,f(x)$ for sufficiently large values of $x$ |
| $\forall$ | For all |
| $p^k \Vert n$ | $p^k$ divides $n$, but $p^{k+1}$ does not divide $n$ |
| $\lvert A\rvert$ | The number of elements in the set $A$ |
| $a \in A$ | $a$ is an element of the set $A$ |
| $a \notin A$ | $a$ is not an element of the set $A$ |
| $a \mid b$ | $a$ divides $b$ |
| $a \nmid b$ | $a$ does not divide $b$ |
| $\pi(x)$ | Number of primes not exceeding $x$ |
| $a \equiv b \pmod{m}$ | $a$ is congruent to $b$ modulo $m$ |
| $a \not\equiv b \pmod{m}$ | $a$ is incongruent to $b$ modulo $m$ |
| $F_n$ | $n$th Fermat number, $F_n = 2^{2^n} + 1$ |

| | |
|---|---|
| $(u,v) \equiv (s,r) \pmod{n}$ | Denote $u \equiv s \pmod{n}$ and $v \equiv r \pmod{n}$ |
| $P(r)$ | The product of distinct prime factors of $r$, for any integer $r > 1$ |
| $\prod_{i=k}^{m} a_i$ | $a_k a_{k+1} \cdots a_m$ |
| $gcd(a,b)$ | The greatest common divisor of $a$ and $b$ |
| $\phi(n)$ | Euler phi function |
| $ord_m a$ | order of $a$ modulo $m$ |
| $ind_r a$ | Index of $a$ relative to $r$ |
| $\left(\frac{a}{p}\right)$ | Legendre symbol ($p$ is odd prime) |
| $\left(\frac{a}{b}\right)$ | Jacobi symbol |
| $\blacksquare$ | End of the proof |

**PERSAMAAN DIOPHANTINE: KONJEKTUR JEŚMANOWICZ DAN KES-KES KHAS TERPILIH**

## ABSTRAK

Pada tahun 1956, Jeśmanowicz mengatakan bahawa untuk sebarang rangkap tiga Pithagorasan primitif $(a,b,c)$ dengan persamaan Diophantine $a^2 + b^2 = c^2$ dan untuk sebaran g integer positif $k$, satu-satunya penyelesaian persamaan $(ak)^x + (bk)^y = (ck)^z$, dalam integer positif, adalah $(x,y,z) = (2,2,2)$. Ini adalah satu konjektur yang tidak dapat diselesaikan bagi rangkap tiga Pithagorasan dan persamaan Diophantine eksponen, dan secara amnya, ia belum dapat diselesaikan. Tesis ini mengandungi enam bab. Bab pertama adalah mengenai pengenalan tesis. Bab 2 adalah tinjauan awal dan tinjauan literatur. Bab 3,4 dan 5 adalah hasil dapatan kajian. Dalam Bab 3, kami memberikan hasil dapatan baharu dan kes-kes khas yang baharu bagi konjektur Jeśmanowicz' bagi rangkap tiga Pithagorasan primitif $(a,b,c) = (4n, 4n^2 - 1, 4n^2 + 1)$ apabila $n = 20$ dan $n = 33$. Dalam Bab 4, kami memberikan hasil baharu dan kes-kes khas yang baharu bagi konjektur Jeśmanowicz' bagi rangkap tiga Pithagorasan primitif $(a,b,c) = (4n^2 - 1, 4n, 4n^2 + 1)$ dan untuk kes khas yang tidak terhingga dengan beberapa syarat apabila $n = p_1^{2r_1} p_2^{2r_2} p_3^{2r_3}$ dan $n = 2^\alpha p^\beta$, yang mana $p, p_1, p_2, p_3$ adalah bilangan nombor perdana yang lebih besar daripada 3 dengan $p_1, p_2, p_3$ adalah berbeza diantara satu sama lain, dan $r_1, r_2, r_3, \alpha, \beta$ adalah integer positif. Tambahan lagi, dalam Bab 5 kajian ini bertujuan untuk memberikan dua pengitlakan untuk persamaan $x^a + y^a = p^k z^b$. Pengitlakan pertama ialah persamaan $x_1^{a_1} + x_2^{a_2} + \cdots + x_m^{a_m} = ny^b$, yang mana $a_i$, $(i = 1,2,3,\ldots,m), b, n, m$ adalah integer positif, tidak mempunyai penyelesaian integer bukan sifar $(x_1, x_2, \ldots, x_m, y)$, sekiranya syarat-syarat tertentu dipenuhi. Pengitlakan

kedua melibatkan persamaan $x_1^a + x_2^a + \cdots + x_m^a = p^k y^b$, yang mana $a, b, k$ adalah integer positif, $gcd(a,b) = 1$ dengan $m$ dan $p$ adalah nombor-nombor perdana dan $x_1, x_2, \ldots, x_m, y$ adalah integer, diselesaikan secara parametrik sekiranya syarat-syarat tertentu dipenuhi.

**ON THE DIOPHANTINE EQUATION: JEŚMANOWICZ CONJECTURE AND SELECTED SPECIAL CASES**

## ABSTRACT

In 1956, Jeśmanowicz conjectured that for any primitive Pythagorean triple $(a,b,c)$ with the Diophantine equation $a^2+b^2=c^2$ and any positive integer $k$, the only solution of equation $(ak)^x+(bk)^y=(ck)^z$, in positive integers, is $(x,y,z)=(2,2,2)$. It is a famous unsolved conjecture on Pythagorean triples and exponential Diophantine equations, and generally it has not been solved yet. In this thesis, there are six chapters all together. The first chapter is on introduction of the thesis. Chapter 2 represents preliminaries and literature review. Chapters 3,4 and 5 are the result chapters. In Chapter 3, we provide new results and special cases on the Jeśmanowicz'conjecture for primitive Pythagorean triple $(a,b,c)=(4n,4n^2-1,4n^2+1)$ when $n=20$ and $n=33$. In Chapter 4, we provide results and special cases on the Jeśmanowicz' conjecture when $(a,b,c)=(4n^2-1,4n,4n^2+1)$ for infinite special cases under some conditions when $n=p_1^{2r_1}p_2^{2r_2}p_3^{2r_3}$ and $n=2^{\alpha}p^{\beta}$, where $p,p_1,p_2,p_3$ are primes that are greater than 3 with $p_1,p_2,p_3$ distinctive and $r_1,r_2,r_3,\alpha,\beta$ are positive integers. Moreover, in Chapter 5 the study aims to provide two generalizations for equation $x^a+y^a=p^kz^b$. The first generalization is that the equation $x_1^{a_1}+x_2^{a_2}+\cdots+x_m^{a_m}=ny^b$, where $a_i$, $(i=1,2,3,\ldots,m),b,n,m$ are positive integers, has no non-zero integral solutions $(x_1,x_2,...,x_m,y)$ if certain conditions are satisfied. The second generalization involves the equation $x_1^a+x_2^a+\cdots+x_m^a=p^ky^b$, where $a,b,k$ are positive integers, $gcd(a,b)=1$ with $m$ and $p$, are primes, and $x_1,x_2,\ldots,x_m,y$ are integers, is solved parametrically if certain conditions are satisfied.

# CHAPTER 1

# INTRODUCTION

## 1.1 History of Diophantus

Diophantine equation is an equation that requires integers to be the solutions. This section discuss about the history of an ancient Mathematician, named Diophantus of Alexandria that had brought in the idea of Diophantine equations. Diophantus had written a series of books entitled Arithmetica. He is widely known as the “father of algebra”, see Andreescu, Andrica and Cucurezeanu (2010) and Jones (1997). In his book, solutions to algebraic equations are discussed. The ‘numbers’ theory in Arithmetica is also discussed in the book. Little is known, however, about his life, and even though Diophantus lived during the Silver era, it is difficult to detect his life span exactly. Therefore, there has been much debate and uncertainty about how long his life span was. He wrote ‘Arithmetica’ in Alexandria, the well-known city for learning mathematics. During the Silver Age or the Later Alexandrian Age, mathematicians discovered numerous ideas and concepts, which paved the way for our conception of mathematics today. The Silver Age is known as the Silver era because it followed the Golden era of significant developments in mathematics. Euclid has lived during the Golden Age. The developments, which occurred during the Golden era, have led to the axiomatic approaches of today’s mathematics. Countless references have been made to the Diophantus’ famous book by other scholars. However, he cited few works of previous mathematicians, which makes it difficult to track down his life span.

Diophantus defined the polygonal number based on Hypsicles' work, who was highly productive before 150 BCE. Therefore, it can be concluded that Diophantus lived in the subsequent period. Moreover, another mathematician from Alexandria named Theon has quoted Diophantus' work in 350 CE. Historians suggested that Diophantus produced many of his works around 250 CE. A considerable amount of knowledge about Diophantus' life was possibly originated based on a fictional collection of riddles. These are known as the Metrodorus' riddles. They were written in 500 CE. The following riddle is an example of the Metrodorus' riddles:

*His boyhood lasted 1/6 of his life span. He got married after 1/7. His beard grew after 1/12. Five years later, his son was born, whose life span continued until his father's half age, the father passed away four years later.*

Furthermore, Diophantus is the first mathematician, who implemented symbols in Greek algebra. He employed the symbol of (arithmos) for a specific quantity that is unknown. He also used symbols for algebraic operations in addition to symbols for powers. Arithmetica is a significant work because of the results in the theory of numbers, including the fact that no integer of the form $8n+7$ can be used as three squares' sum. Arithmetica includes a collection of 150 problems, which can provide estimated equations' solutions up to degree three. Additionally, Arithmetica involves equations pertaining to indeterminate equations, which are relevant to the theory of numbers.

It is believed that the original version of Arithmetica consisted of 13 books. However, the existing Greek manuscripts include only six; the remaining books are regarded as lost works. It is believed that these books were lost because of a fire that broke out shortly after Diophantus finished writing Arithmetica. Therefore, the Diophantine equation is called an 'equation of the form'

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{1.1}$$

where $f$ is an $n$-variable function with $n \geqslant 2$. If $f$ is a polynomial with integral coefficients, then (1.1) is an algebraic Diophantine equation and $f$ is exponential Diophantine if $f$ is exponential polynomial.

An $n$-uple $(x_1^0, x_2^0, \ldots, x_n^0) \in \mathbb{Z}^n$ satisfying (1.1) is called a solution to Equation (1.1). An equation, which has a single solution or a range of solutions, is called a solvable equation. Regarding the Diophantine equation, three fundamental problems can be postulated as follows:

**Problem 1**. Can the equation be solved?

**Problem 2.** If the equation can be solved, is the number of potential solutions to the equation finite or infinite?

**Problem 3.** If the equation can be solved, identify all the potential solutions to the equation.

The work of Diophantus about equations of type (1.1) has been continued by Chinese mathematicians (during the third century) and Arabs (during the eighth century through the twelfth century). Moreover, the Diophantus' work was meticulously continued by Fermat, Euler, Lagrange, Gauss, and many others. In contemporary mathematics, the works of Diophantus are particularly significant.

The theory of Diophantine equations has been known for many years, and it has attracted the attention of many scholars in Number theory and Cryptography. Moreover, the Diophantine equation problem constitutes the most popular problem, which is debated and discussed among mathematicians and computer scientists. As the concept of cryptography evolved around solving computationally hard mathematical problems, therefore solving equations to find rational and integral solutions is regarded as one of many preferred problems in Cryptography. More importantly and in a broader sense, solving Diophantine equations can be perceived as solving Diophantine geometry problems that lead to the idea of solving elliptic curve equations in elliptic curve cryptography (ECC). ECC is based on the calculations in the finite field for a Diophantine equation of degree 3 or more in two variables. Another cryptographic idea of the Diophantine equation problem involves solving multivariate equations that are multivariate functions or polynomials defined in the algebraic field. Accordingly, in addition to what has been discovered from the Jeśmanowicz' conjecture, several more results are obtained in this study to solve certain types of Diophantine equations. The results contribute to establishing and enhancing fundamental ideas, which can hopefully be useful for solving hard-mathematical problems in cryptography and other fields in Mathematics.

## 1.2 Leon Jeśmanowicz (1914-1989)

Figure 1.1: Jeśmanowicz[1]

On the twenty-seventh of April 1914, Prof. Leon Jeśmanowicz was born in Druja city in the region of Vilnius, see (Jeśmanowicz, 1994) and (Soydan, Demirci, Cangul and Togbé, 2017). His father Anatole Jeśmanowicz worked as a clerk in a post office and his mother's name is Irene. In 1920, the family moved to Vilnius, where his father passed away. His mother moved to Łodzi first and after that to Grodno. In 1932, Jeśmanowicz completed secondary school to pursue his study in humanities. From 1933 until 1937, Jeśmanowicz studied Maths at the University of Stefan Batory in Vilnius. During his first two years of studying Math, Jeśmanowicz also studied painting at the Fine Arts Faculty. After he graduated from university, he was granted a scholarship, which was awarded by the National Culture Fund and, thus, Jeśmanowicz started his career as a junior university assistant. During the Second World War, he worked as an assistant at the Department of Mathematics under Prof. Antoni Zygmund's supervision. In 1939, Jeśmanowicz completed writing his doctoral dissertation. However, he could not defend it due to the outbreak of World War II. Jeśmanowicz conducted clandestine study groups during the German occupation. In March 1945, he returned to Lublin with his family. There, he was offered a position at the Department of Mathematics / University of Maria Curie-Skłodowska. In July 1945, Jeśmanowicz could finally defend his dissertation on the Schlömilcha series uniqueness under Prof. Juliusz Rudnicki's supervision. In October 1945, Jeśmanowicz

[1] Jeśmanowicz online family album (https://www.jesmanowicz.com)

was appointed as a senior university assistant. A year later, he settled in Torun. There, he worked in the newly established Mathematics Department at Nicolaus Copernicus University until he passed away in1989. Jeśmanowicz held the position of Assistant Professor in 1949 and Associate Professor in 1954. Ten years later, he was awarded a Full Professor title by the State Council. Jeśmanowicz held many academic positions in Faculties of Maths, Physics, and Chemistry, including Vice Dean and Dean. Many social duties were also fulfilled by him; he was a long-established chairperson of the Torun branch of the Polish Mathematical Society and a boarding committee member. His outstanding achievements included the investigation of the theory of Sumawalności ranks, the abelian groups' theory, and the Diophantine equations' solutions. In addition to Mathematics, Prof. Jeśmanowicz's interests included literature, history, theatre, and caricature. In his paintings, Jeśmanowicz depicted his experiences with hundreds of people and groups during his life.

### 1.3 The Jeśmanowicz' Conjecture

Jeśmanowicz (1955/1956) conjectured that the exponential Diophantine equation

$$(ak)^x + (bk)^y = (ck)^z, \qquad x, y, z \in \mathbb{N} \tag{1.2}$$

has a unique solution $(x, y, z) = (2, 2, 2)$ for any positive integer $k$, where $(a, b, c)$ are primitive Pythagorean triple. It is a famous unsolved conjecture on Pythagorean triples and exponential Diophantine equations, and it has been solved for special cases. Generally, the conjecture has not been solved so far. In fact, Equation (1.2) has a long history and many mathematicians studied it, see (Ma and Chen, 2017), (Han and Yuan, 2018), (Deng and Huang, 2017), (Hu and Le, 2018), (Soydan *et al*., 2017), (Deng and Guo, 2017), (Yuan and Han, 2018), (Yang and Fu, 2019), (Fu and Yang, 2020) and (Le and Soydan, 2020).

Sierpiński (1955/1956) showed that the conjecture is true for $k = 1$ and $(a,b,c) = (3,4,5)$, i.e., the equation

$$3^x + 4^y = 5^z, \tag{1.3}$$

has no positive integer solutions other than $(x,y,z) = (2,2,2)$. Jeśmanowicz has also proved the same result and other special cases, where Jeśmanowicz (1955/1956) proved that the conjecture is true for the following special Diophantine equations

$$\begin{aligned} (5)^x + (12)^y &= (13)^z, \\ (7)^x + (24)^y &= (25)^z, \\ (9)^x + (40)^y &= (41)^z, \\ (11)^x + (60)^y &= (61)^z. \end{aligned} \tag{1.4}$$

There are many special cases of the Jeśmanowicz' conjecture that are solved for $k = 1$. Yang and Tang (2012) proved that the only solution of the Diophantine equation

$$(8k)^x + (15k)^y = (17k)^z, \tag{1.5}$$

is given by $(x,y,z) = (2,2,2)$, for $k \geqslant 1$. Yang and Weng (2012) proved that the only solution of the Diophantine equation

$$(12k)^x + (35k)^y = (37k)^z, \tag{1.6}$$

is $(x,y,z) = (2,2,2)$ where $k \geqslant 1$. Several authors have shown that the Jeśmanowicz's conjecture is true for $n \in \{2,4,8\}$ and $k > 1$, where $(a,b,c) = (4n, 4n^2-1, 4n^2+1)$, see (Tang and Weng, 2014) and (Tang and Yang, 2013).

Ma and Wu (2015) proved that the only solution of the Diophantine equation

$$((4n^2-1)k)^x + (4nk)^y = ((4n^2+1)k)^z, \tag{1.7}$$

is given by $(x,y,z) = (2,2,2)$ when $P(4n^2-1)|k$, (where $P(r)$ denotes the product of distinct prime of $r$, for any positive integer $r$ is greater than 1). They also showed that if $k$ is a positive integer, and $P(k) \nmid (4n^2-1)$, then the only solution of Equation (1.7) is $(x,y,z) = (2,2,2)$. In this case, they considered $n = p^m$, where $m \geqslant 0$ and $p$ is a prime such that $p \equiv 3 \pmod 4$. Soydan *et al.* (2017) considered Equation (1.2) with $(a,b,c) = (20,99,101)$ and they proved that the Diophantine equation

$$(20k)^x + (99k)^y = (101k)^z, \tag{1.8}$$

has only the solution $(x,y,z) = (2,2,2)$. They considered the case $n = 5$ and $(a,b,c) = (4n, 4n^2-1, 4n^2+1)$ for Equation (1.2). For other results, see (Tang and Yang, 2013), (Sun and Cheng, 2015), (Le, 1999) and (Deng and Cohen, 1998). Motivated by all of these results, we study the Jeśmanowicz' conjecture and certain types of the Diophantine equation are introduced and studied and new results with their proofs are provided in Chapters 3, 4 and 5.

## 1.4 The Diophantine Equation $x^a + y^a = p^k z^b$

Diophantine equations have attracted the mathematicians' attention for more than 3 centuries. Looking back at the history of Fermat's Last Theorem in the following equation:

$$x^n + y^n = z^n, \tag{1.9}$$

where it stipulates that if $n$ is an integer greater than 2, then Equation (1.9) has no solution in positive integers $x, y$, and $z$. This equation has given rise to many variations of similar forms with restrictions and conditions. Taylor and Wiles (1995) and Wiles (1995) established the modularity of a large class of curves in 1995 that has led to the accomplishment of the Fermat's problem (Narkiewicz, 2012) and (Cornell, Silverman and Stevens, 1997). Apart from the ideas and results on solving Equation (1.9), many results have been established on equations related to it. With a different exponent on the right-hand side of Equation (1.9), Wong and Kamarulhaili (2016) partially solved the Diophantine equation

$$x^4 + y^4 = p^k z^7, \tag{1.10}$$

where $p$ is a prime and $k$ is a positive integer for when $x = y$. Wong and Kamarulhaili (2017) studied a more general form of Equation (1.10) in the following equation:

$$x^a + y^a = p^k z^b, \tag{1.11}$$

where $p$ is a prime number, with $\gcd(a,b) = 1$ and $k, a, b \in \mathbb{N}$. They solved this equation parametrically by considering different cases of $x$ and $y$ for when $x = y$, $x = -y$, and either $x$ or $y$ is zero (not both zero). They also considered the case when, $|x| \neq |y|$ and both $x$ and $y$ are non-zero, but in this case, only partial solutions of $(x,y,z)$ were given. The work by Wong and Kamarulhaili has triggered an idea to extend Equation (1.11) to a summation form. Given the summation form of Equation (1.11), the results provided by Bérczes, Hajdu, Miyazaki and Pink (2016) and Bérczes, Pink, Sava¸s and Soydan (2018) are consistent. Bérczes *et al*. (2016) provided all the solutions of the equation

$$S_k(x) = 1^k + 2^k + \cdots + x^k = y^n, \tag{1.12}$$

in positive integers $x,k,y,n$ with $1 \leqslant x < 25$ and $n \geqslant 3$. Bérczes *et al*. (2018), gave upper bounds for $n$ on the Diophantine equation

$$(x+1)^k + (x+2)^k + \cdots + (2x)^k = y^n, \tag{1.13}$$

and showed that for $2 \leqslant x \leqslant 13,\ k \geqslant 1,\ y \geqslant 2$, and $n \geqslant 3$, Equation (1.13) does not have solutions. Based on the previous works, a different form of the equation is provided in this study, given as $x_1^{a_1} + x_2^{a_2} + \cdots + x_m^{a_m} = ny^b$, where $a_i,\ (i = 1,2,3,...,m), b,n,m$ are positive integers. The aim is to prove that under some conditions, the above equation has no non-zero integral solutions $x_1, x_2, \ldots, x_m$, and $y$. Moreover, the implications of the results, which are related to Equation (1.12), are provided and discussed. Also, a different form of the equation is given as, $x_1^a + x_2^a + \cdots + x_m^a = p^k y^b$ for $a,b,k$ are positive integers and $p$ is arbitrary prime. With some conditions, the results of solving this equation are provided in (**Section** 5.2).

## 1.5 Problem Statement

This study addresses one of the most famous unsolved conjectures in the field of Diophantine equations. The exponential Diophantine equation $(ak)^x + (bk)^y = (ck)^z$ has the unique solution $(x,y,z) = (2,2,2)$ for any positive integer $k$ with $(a,b,c)$, which is primitive Pythagorean triple, where $x, y$, and $z$ are positive integers. This conjecture is called the Jeśmanowicz' conjecture (Jeśmanowicz, 1955/1956). Moreover, certain types of Diophantine equations are addressed in this study to provide a generalization to the equation $x^a + y^a = p^k z^b$ (Wong and Kamarulhaili, 2016) and (Wong and Kamarulhaili, 2017).

## 1.6 Research Objectives

(i) To provide new results and special cases on the Jeśmanowicz' conjecture for primitive Pythagorean triple $(a,b,c) = (4n, 4n^2 - 1, 4n^2 + 1)$ without conditions.

(ii) To prove that the Jeśmanowicz' conjecture is true for infinite special cases of the Pythagorean triple $(a,b,c) = (4n^2 - 1, 4n, 4n^2 + 1)$ with some conditions.

(iii) To generalize the Diophantine equation $x^a + y^a = p^k z^b$ to the Diophantine equation in several variables $x_1^a + x_2^a + \cdots + x_m^a = p^k y^b$ with some conditions.

(iv) To investigate the Diophantine equation $x_1^{a_1} + x_2^{a_2} + \cdots + x_m^{a_m} = ny^b$ and relate it with the prime numbers with some conditions.

## 1.7 Research Methodology

To achieve the objectives of the study, several definitions, theorems, prepositions, lemmas were taken from the second chapter and applied throughout the research. In addition, some useful results from previous studies are also used. In Chapter three, the results of the following studies (Le, 1999), (Lu, 1959), (Deng and Cohen, 1998) and (Deng, 2014) were used. In Chapter four, the results of the studies Ma and Wu (2015), (Deng, 2014) and (Lu, 1959) were utilized. And finally, in Chapter five the Fermat's Method of Infinite Descent, as well as the results of (Wong and Kamarulhaili, 2016) and (Wong and Kamarulhaili, 2017) were used to obtain the desired results.

## 1.8 Thesis Organization

The thesis is organized into six chapters as follows:

**Chapter 1** introduces the topic of the study about the Jeśmanowicz' conjecture and certain types of Diophantine equations. It provides the statement of the problem, the research objectives, and the implemented methodology of the study. The chapter ends with the organization of the thesis.

**Chapter 2** provides the basic concepts in number theory, including definitions, theorems, lemmas, and propositions. This chapter reviews previous studies about the Jeśmanowicz' conjecture and provides several results related to the conjecture, which are used in this study. This chapter also reviews the conducted studies about certain types of the Diophantine equation.

**Chapter 3** gives preliminary results, along with two main new results on the conjecture for Pythagorean triples $(a,b,c) = (4n, 4n^2-1, 4n^2+1)$. The first main result as a special case when $n = 20$ and it has been proven that the conjecture is true in this case, i.e., the only positive integer solution of equation $(80k)^x + (1599k)^y = (1601k)^z$ is $(x,y,z) = (2,2,2)$, for every positive integer $k$. The second main result is another special case when $n = 33$. It has been proven that the conjecture is true in this case, i.e., the only positive integer solution of equation $(132k)^x + (4355k)^y = (4357k)^z$ is $(x,y,z) = (2,2,2)$, for every positive integer $k$.

**Chapter 4** provides preliminary results with two main results, including the third and the fourth main results on the conjecture for Pythagorean triples $(a,b,c) = (4n^2 - 1, 4n, 4n^2 + 1)$ when certain divisibility conditions are satisfied. Regarding the third main result, it is assumed that $p_1, p_2, p_3$ distinctive primes greater than 3 and $r_1, r_2, r_3$ are positive integers, which showed that the conjecture is true for $n = p_1^{2r_1} p_2^{2r_2} p_3^{2r_3}$. Regarding the fourth main result, it is assumed that $p$ is arbitrary prime greater than 3 and $\alpha, \beta$ are positive integers and $y$ belongs to the set of even positive, which showed that the conjecture is true for $n = 2^{\alpha} p^{\beta}$.

**Chapter 5** preliminary results and 3 main results to extend the equation $x^a + y^a = p^k z^b$ to a summation form under some conditions. Regarding the first main result, we proved that equation $x_1^{a_1} + x_2^{a_2} + \cdots + x_m^{a_m} = ny^b$, has no non-zero integral solutions $(x_1, x_2, ..., x_m, y)$. Regarding the second and third main results, the formulated parametric solutions are provided to solve the equation $x_1^a + x_2^a + \cdots + x_m^a = p^k y^b$, where we proved the existence of many infinitely nontrivial integer solutions. Additionally, implications and some examples are provided in this chapter.

**Chapter 6** provides conclusions of this study and advances recommendations for further studies.

# CHAPTER 2

# PRELIMINARIES AND LITERATURE REVIEW

## 2.1 Introduction

The basic concepts on number theory are provided in this chapter. Previous studies on Jeśmanowicz' conjecture and selected Diophantine equations are reviewed in this chapter.

## 2.2 Basic Concepts

This section introduces some basic concepts on number theory, which are used in Chapters 3, 4 and 5. The main references of this section are (Andreescu *et al*., 2010), (Strayer, 2002) and (Koshy, 2007).

**Definition 2.2.1 (Division)** *(Strayer, 2002). Suppose that $a$ and $b$ are integers. We say that $a$ divides $b$, written $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$. The notation $a \nmid b$, if there is no $c \in \mathbb{Z}$ such that $b = ac$.*

**Theorem 2.2.1 (The Division Algorithm)** *(Strayer, 2002). For any integer $a$ and $b \in \mathbb{N}$. Then, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$, with $0 \leq r < b$.*

**Definition 2.2.2 (Greatest Common Divisor (gcd))** *(Fine and Rosenberger, 2007). Suppose that $a$ and $b$ are non-zero integers. The greatest common divisor of $a$ and $b$, denoted by $gcd(a,b)$ or $(a,b)$, is the positive integer $d$ satisfying $d|a$ and $d|b$, and* *if $d_1 \mid a$ and $d_1 \mid b$, then $d_1 \mid d$. If $gcd(a,b) = 1$, then we consider that a and b are relatively prime.*

**Proposition 2.2.1** *(Coppel, 2009). $\forall a,b,c \in \mathbb{N}$ and $gcd(a,b) = 1$, then*

*(i) if $a \mid c$ and $b \mid c$, then $ab \mid c$,*

*(ii) if $a \mid bc$, then $a \mid c$,   (Euclid's Lemma)*

*(iii) $gcd(a,cb) = gcd(a,c)$,*

*(iv) if $gcd(a,c) = 1$, then $gcd(a,bc) = 1$,*

*(v) $gcd(a^m,b^n) = 1$ for all $m,n \geq 1$.*

**Definition 2.2.3 (Prime and Composite)** *(Strayer, 2002)An integer n greater than 1 is prime if its only positive divisors are 1 and n. We call n composite if it is not prime.*

**Corollary 2.2.1** *(Strayer, 2002)If $p \mid (a_1a_2\cdots a_n)$, then $p \mid a_i$ for some i, where $a_1,a_2,\ldots,a_n$ be integers and p be a prime.*

**Remark 2.2.1** *(Strayer, 2002)Let $gcd(a,b) = 1$. Then, $gcd(a+b,a-b)$ is either* 1 *or* 2*.*

**Lemma 2.2.1** *(Fine and Rosenberger, 2007). Let c be an integer. Then, $gcd(a,b) = gcd(a,b+ac)$.*

**Theorem 2.2.2 (Fundamental Theorem of Arithmetic)** *(Strayer, 2002)*

*Every integer greater than 1 can be expressed in the form* $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ *with* $p_1, p_2, \ldots, p_n$ *distinct prime numbers and* $a_1, a_2, \ldots, a_n$ *positive integers. This prime factorization is unique except for the arrangement of the* $p_i^{a_i}$.

**Lemma 2.2.2** *(Rosen, 2011). If a and b are positive integers such that* $gcd(a,b) = 1$. *Then, if* $c \mid ab$, *where c is positive, there is a unique pair of positive divisors* $c_1$ *of a and* $c_2$ *of b such that* $c = c_1c_2$. *Conversely, if* $c_1 \mid a$ *and* $c_2 \mid b$, *where* $c_1$ *and* $c_2$ *are positive, then* $c = c_1c_2 \mid ab$.

**Definition 2.2.4** *(Strayer, 2002)Let x be a positive real number, then* $\pi(x)$ *is a function defined by*

$$\pi(x) = |\{p : p \text{ prime; } 1 < p \leqslant x\}|.$$

**Theorem 2.2.3 (Prime Number Theorem)** *(Strayer, 2002)*

$$\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1.$$

**Definition 2.2.5** *(Rosen, 2011). Let* $a, b, m$ *are integers with* $m > 0$. *Then,* $a \equiv b(\bmod m)$, *we say (a is congruent to b modulo m) if* $m|a-b$.

**Proposition 2.2.2** *(Strayer, 2002). If* $a, b, c$ *are integers and n is a positive integer, then* $ac \equiv bc(\bmod n)$ *if and only if* $a \equiv b(\bmod (n/gcd(n,c)))$.

**Theorem 2.2.4 (Fermat's Little Theorem)** *(Strayer, 2002). Let p be a prime number and* $a \in \mathbb{Z}$ *for which the* $gcd(a, p) = 1$. *Then, it holds* $a^{p-1} \equiv 1(\bmod p)$.

**Definition 2.2.6 (Quadratic Residue)** *(Strayer, 2002). An integer a is called a quadratic residue modulo b, where b is a positive integer, if* $gcd(a,b) = 1$ *and the congruence* $x^2 \equiv a \pmod{b}$ *is solvable in* $\mathbb{Z}$*; otherwise, it is a quadratic nonresidue modulo b.*

**Definition 2.2.7 (Legendre Symbol)** *(Strayer, 2002). Let p be an odd prime number and a is an integer with* $p \nmid a$*. The Legendre symbol* $\left(\frac{a}{p}\right)$ *is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{otherwise.} \end{cases}$$

**Theorem 2.2.5** *(Strayer, 2002). Let p be an odd prime number. Then,*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv 1,7 \pmod{8} \\ -1, & \text{if } p \equiv 3,5 \pmod{8} \end{cases}$$

**Remark 2.2.2** *(Rosen, 2011). Let p be an odd prime number. Then,*

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1,3 \pmod{8} \\ -1, & \text{if } p \equiv 5,7 \pmod{8} \end{cases}$$

**Definition 2.2.8 (Jacobi Symbol)** *(Strayer, 2002). Let n be an odd positive integer greater than 1, and a is an integer with* $gcd(n,a) = 1$ *and let the prime factorization of n is* $\prod_{i=1}^{r} p_i^{b_i}$*. The Jacobi symbol, denoted* $\left(\frac{a}{n}\right)$*, is*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{b_i},$$

*where,* $\left(\frac{a}{p_1}\right), \left(\frac{a}{p_2}\right), \ldots, \left(\frac{a}{p_r}\right)$ *are Legendre symbols.*

**Definition 2.2.9 (The Euler Phi-Function)** *(Strayer, 2002). Let n be a positive integer. Then, the Euler phi-function $\phi(n)$ is the function defined by*

$$\phi(n) = |\{x \in \mathbb{Z} : 1 \leqslant x \leqslant n;\ gcd(x,n) = 1\}|.$$

**Theorem 2.2.6 (Euler's Theorem)** *(Strayer, 2002). If $gcd(a,m) = 1$, then*

$$a^{\phi(m)} \equiv 1(\bmod m),$$

*where m be a positive integer and a be an integer.*

**Definition 2.2.10** *(Rosen, 2011). Let $a, m \in \mathbb{Z}$ with $m > 0, a \neq 0$ and $gcd(a,m) = 1$. Then, the least positive integer x such that*

$$a^x \equiv 1(\bmod m),$$

*is called the order of a modulo m, denoted by $ord_m a$.*

**Theorem 2.2.7** *(Rosen, 2011). If $a \in \mathbb{Z}, a \neq 0$ and $n \in \mathbb{N}$ with $gcd(a,n) = 1$. Then, the positive integer x is a solution of the congruence $a^x \equiv 1(\bmod n)$ if and only if $ord_n a \mid x$.*

**Definition 2.2.11 (Primitive Root)** *(Strayer, 2002). If $gcd(a,n) = 1$ and $n > 0$ with*

$$ord_n a = \phi(n).$$

*Then, a is called a primitive root modulo n.*

**Example 2.2.1** *(Koshy, 2007). Table 2.1 illustrates the smallest primitive root modulo each prime* $p < 312$

Table 2.1: The smallest primitive root modulo each prime $p < 312$

| $p$ | Primitive Root | $p$ | Primitive Root | $p$ | Primitive Root | $p$ | Primitive Root |
|---|---|---|---|---|---|---|---|
| 2 | 1 | 59 | 2 | 137 | 3 | 227 | 2 |
| 3 | 2 | 61 | 2 | 139 | 2 | 229 | 6 |
| 5 | 2 | 67 | 2 | 149 | 2 | 233 | 3 |
| 7 | 3 | 71 | 7 | 151 | 6 | 239 | 7 |
| 11 | 2 | 73 | 5 | 157 | 5 | 241 | 7 |
| 13 | 2 | 79 | 3 | 163 | 2 | 251 | 6 |
| 17 | 3 | 83 | 2 | 167 | 5 | 257 | 3 |
| 19 | 2 | 89 | 3 | 173 | 2 | 263 | 5 |
| 23 | 5 | 97 | 5 | 179 | 2 | 269 | 2 |
| 29 | 2 | 101 | 2 | 181 | 2 | 271 | 6 |
| 31 | 3 | 103 | 5 | 191 | 19 | 277 | 5 |
| 37 | 2 | 107 | 2 | 193 | 5 | 281 | 3 |
| 41 | 6 | 109 | 6 | 197 | 2 | 283 | 3 |
| 43 | 3 | 113 | 3 | 199 | 3 | 293 | 2 |
| 47 | 5 | 127 | 3 | 211 | 2 | 307 | 5 |
| 53 | 2 | 131 | 2 | 223 | 3 | 311 | 17 |

**Definition 2.2.12 (Index)** *(Burton, 2011). Let r be a primitive root of n, and a is an arbitrary integer such that* $gcd(a,n) = 1$. *Then, the smallest positive integer k such that* $a \equiv r^k (\bmod n)$ *is called the index of a relative to r. It is denoted by* $ind_r a$ *or* $ind\, a$.

**Example 2.2.2** *(Koshy, 2007). Table 2.2 illustrates Indices for the prime 13 relative to the primitive root 2*

Table 2.2: Indices for the prime 13 relative to the primitive root 2

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{ind}_2 a$ | 12 | 1 | 4 | 2 | 9 | 5 | 11 | 3 | 8 | 10 | 7 | 6 |

**Example 2.2.3** *(Koshy, 2007). Table 2.3 illustrates Indices for the prime 5 relative to the primitive root 2*

Table 2.3: Indices for the prime 5 relative to the primitive root 2

| $a$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $\mathrm{ind}_2 a$ | 4 | 1 | 3 | 2 |

**Example 2.2.4** *(Koshy, 2007). Table 2.4 illustrates Indices for the prime 41 relative to the primitive root 6 and Table 2.5 illustrates Indices for the prime 67 relative to the primitive root 2*

Table 2.4: Indices for the prime 41 relative to the primitive root 6

| $a$ | $\text{ind}_6 a$ | $a$ | $\text{ind}_6 a$ |
|---|---|---|---|
| 1 | 40 | 21 | 14 |
| 2 | 26 | 22 | 29 |
| 3 | 15 | 23 | 36 |
| 4 | 12 | 24 | 13 |
| 5 | 22 | 25 | 4 |
| 6 | 1 | 26 | 17 |
| 7 | 39 | 27 | 5 |
| 8 | 38 | 28 | 11 |
| 9 | 30 | 29 | 7 |
| 10 | 8 | 30 | 23 |
| 11 | 3 | 31 | 28 |
| 12 | 27 | 32 | 10 |
| 13 | 31 | 33 | 18 |
| 14 | 25 | 34 | 19 |
| 15 | 37 | 35 | 21 |
| 16 | 24 | 36 | 2 |
| 17 | 33 | 37 | 32 |
| 18 | 16 | 38 | 35 |
| 19 | 9 | 39 | 6 |
| 20 | 34 | 40 | 20 |

Table 2.5: Indices for the prime 67 relative to the primitive root 2

| $a$ | $\text{ind}_2 a$ | $a$ | $\text{ind}_2 a$ | $a$ | $\text{ind}_2 a$ |
|---|---|---|---|---|---|
| 1 | 66 | 23 | 28 | 45 | 27 |
| 2 | 1 | 24 | 42 | 46 | 29 |
| 3 | 39 | 25 | 30 | 47 | 50 |
| 4 | 2 | 26 | 20 | 48 | 43 |
| 5 | 15 | 27 | 51 | 49 | 46 |
| 6 | 40 | 28 | 25 | 50 | 31 |
| 7 | 23 | 29 | 44 | 51 | 37 |
| 8 | 3 | 30 | 55 | 52 | 21 |
| 9 | 12 | 31 | 47 | 53 | 57 |
| 10 | 16 | 32 | 5 | 54 | 52 |
| 11 | 59 | 33 | 32 | 55 | 8 |
| 12 | 41 | 34 | 65 | 56 | 26 |
| 13 | 19 | 35 | 38 | 57 | 49 |
| 14 | 24 | 36 | 14 | 58 | 45 |
| 15 | 54 | 37 | 22 | 59 | 36 |
| 16 | 4 | 38 | 11 | 60 | 56 |
| 17 | 64 | 39 | 58 | 61 | 7 |
| 18 | 13 | 40 | 18 | 62 | 48 |
| 19 | 10 | 41 | 53 | 63 | 35 |
| 20 | 17 | 42 | 63 | 64 | 6 |
| 21 | 62 | 43 | 9 | 65 | 34 |
| 22 | 60 | 44 | 61 | 66 | 33 |

**Proposition 2.2.3** *(Strayer, 2002). Let $r$ be a primitive root modulo $n$ and $a, b$ are integers such that $gcd(a,n) = 1 = gcd(b,n)$. Then,*

*(i)* $ind_r 1 \equiv 0(\mod \phi(n))$,

*(ii)* $ind_r r \equiv 1(\mod \phi(n))$,

*(iii)* $ind_r(ab) \equiv ind_r a + ind_r b(\mod \phi(n))$,

*(iv)* $ind_r(a^m) \equiv m\, ind_r a(\mod \phi(n))$, *if $m$ is a positive integer.*

**Remark 2.2.3** *(Rosen, 2011). Let $a,b,c,n \in \mathbb{Z}, n > 0$ and $d = gcd(a,b,n)$. If $d \mid c$. Then, the linear congruence in two variables $ax + by \equiv c(\mathrm{mod} n)$ has exactly $dn$ incongruent solutions. Otherwise, no solutions.*

**Definition 2.2.13** *(Andreescu et al., 2010). An equation of the form*

$$f(x_1, x_2, \ldots, x_n) = 0,$$

*is called a Diophantine equation where, $f$ is an n-variable function with n is greater or equal than 2 and the solution to this equation is an n-tuple $(x_1^0, x_2^0, ..., x_n^0) \in \mathbb{Z}^n$.*

**Theorem 2.2.8** *(Strayer, 2002). Let $d = gcd(a,b)$. If $d \nmid c$. Then, a linear Diophantine equation $ax+by=c$ has no solutions; if $d \mid c$, then the equation has infinite solutions and if $x_0, y_0$ is a particular solution of the equation, then all solutions are*

$$x = x_0 + \left(\frac{b}{d}\right) n,$$

$$y = y_0 - \left(\frac{a}{d}\right) n,$$

*where $n \in \mathbb{Z}$.*

**Axiom 2.2.1 (Well-Ordering Principle)** *(Rosen, 2011) Every nonempty set of non-negative integers has a least element.*

### 2.2.1 Description of Fermat's Method of Infinite Descent

Let $P$ be a property concerning the nonnegative integers and let $(P(n))_{n\geqslant 1}$ be the sequence of propositions, $P(n)$: "$n$ satisfies property $P$". Therefore, the Fermat's method of infinite descent (FMID) can be described as follows: Suppose that $k$ be a non-negative integer. Assume that, for $m$ is an integer greater than $k$ if $P(m)$ is true, then there exists smaller integer $j$ such that $m > j > k$ for which $P(j)$ is true. Then $P(n)$ is false for all $n$ is greater than $k$, i.e., if there is where an $n$ for which $P(n)$ was true, one could construct a sequence $n > n_1 > n_2 > \cdots$ all of which would be greater than $k$, but by the well-ordering principle, we know that the nonnegative integers cannot be decreased indefinitely, particularly as a special case of FMID, there is no sequence of nonnegative integers $n_1 > n_2 > \cdots$ (Andreescu *et al*., 2010).