ON THE SOLVABILITY OF SOME DIOPHANTINE EQUATIONS OF THE FORM $a^x + b^y = z^2$

AMR MOUSTAFA MOHAMED ALY ELSAYED ELSHAHED

UNIVERSITI SAINS MALAYSIA

2022

ON THE SOLVABILITY OF SOME DIOPHANTINE EQUATIONS OF THE FORM $a^x + b^y = z^2$

by

AMR MOUSTAFA MOHAMED ALY ELSAYED ELSHAHED

**Thesis submitted in fulfilment of the requirements
for the degree of
Master of Science**

July 2022

ACKNOWLEDGEMENT

First and foremost, praise to Allah, the Almighty, the Greatest, on whom ultimately we depend for sustenance and guidance. I would like to express my gratitude to Almighty Allah for providing me with the chance and strength to do my research.

I would like to sincerely thank my supervisor Prof. Dr. Hailiza Kamarulhaili, for her guidance, understanding, and patience.

A special thanks to my parents, Moustafa and Magida for their thoughts, love, encouragement, and prayers during this journey, I will be in their debt forever. I also want to thank my sister Fatimah and brothers Mohamed, Mahmod, and Yousuf who supported me during this journey.

I owe a debt of gratitude to my friends in Kombative, particularly Bekzat, Raymond, Vic, and Mook. I thank them for making me feel home.

And finally, I would like to thank Ahmad, Ibrahim, Abdulrahim, and Abdussalam for all of their constant support and encouragement through thick and thin. I thank them for being true brothers.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

$\mathbb{N}$	The set of natural numbers
$\mathbb{Z}$	The set of integers
$a \in b$	a is an element of the set b
$a \notin b$	a is not an element of the set b
$gcd(a,b)$	The greatest common divisor
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
LHS	The left hand side
RHS	The right hand side

PERIHAL PENYELESAIAN BEBERAPA PERSAMAAN DIOPHANTINE BERBENTUK $a^x + b^y = z^2$

ABSTRAK

Persamaan Diophantine $a^x + p^y = z^2$ yang mana p adalah nombor perdana banyak dikaji oleh ahli matematik. Menyelesaikan persamaan jenis ini sering merangkumi Konjektur Catalan dalam proses pembuktian. Di sini, kami mengkaji penyelesaian integer bukan negatif untuk beberapa persamaan Diophantine dari keluarga yang sama. Kami akan menggunakan teorem Mihailescu (yang merupakan pembuktian kepada konjektur Catalan) dan kaedah asas untuk menyelesaikan persamaan Diophantine $16^x - 7^y = z^2$, $16^x - p^y = z^2$ dan $64^x - p^y = z^2$, kemudian kami akan mengkaji suatu generalisasi yang mana $(4^n)^x - p^y = z^2$ dan x, y, z, n adalah bukan integer negatif. Seterusnya, dengan menggunakan teorem Mihailescu dan pendekatan asas dalam teori nombor, iaitu teori kongruen, kami akan menentukan penyelesaian persamaan Diophantine $7^x + 11^y = z^2$, $13^x + 17^y = z^2$, $15^x + 17^y = z^2$ dan $2^x + 257^y = z^2$ yang mana x, y dan z adalah integer bukan negatif. Kami juga akan membuktikan bahawa sebarang nombor bulat bukan negatif n, semua penyelesaian integer bukan negatif daripada persamaan Diophantine $11^n 8^x + 11^y = z^2$ adalah dalam bentuk $(x, y, z) = (1, n, 3(11)^{\frac{n}{2}})$ dengan n genap dan ia tidak mempunyai penyelesaian jika n ganjil. Akhirnya, kami akan menumpukan perhatian untuk mencari penyelesaian kepada persamaan Diophantine $3^x + p^m n^y = z^2$ yang mana $y = 1, 2$ dan $p > 3$ adalah nombor perdana.

ON THE SOLVABILITY OF SOME DIOPHANTINE EQUATIONS OF THE FORM $a^x + b^y = z^2$

ABSTRACT

The Diophantine equation $a^x + p^y = z^2$ where p is prime is widely studied by many mathematicians. Solving equations of this type often include Catalan's conjecture in the process of proving these equations. Here, we study the non-negative integer solutions for some Diophantine equations of such family. We will use Mihailescu's theorem (which is the proof of Catalan's conjecture) and elementary methods to solve the Diophantine equations $16^x - 7^y = z^2$, $16^x - p^y = z^2$ and $64^x - p^y = z^2$, then we will study a generalization where $(4^n)^x - p^y = z^2$ and x, y, z, n are non-negative integers. By using Mihailescu's theorem and a fundamental approach in the theory of numbers, namely the theory of congruence, we will determine the solution of the Diophantine equations $7^x + 11^y = z^2$, $13^x + 17^y = z^2$, $15^x + 17^y = z^2$ and $2^x + 257^y = z^2$ where x, y and z are non-negative integers. Also, we will prove that for any non-negative integer n, all non-negative integer solutions of the Diophantine equation $11^n 8^x + 11^y = z^2$ are of the form $(x, y, z) = (1, n, 3(11)^{\frac{n}{2}})$ where n is even, and has no solution when n is odd. Finally, we will concentrate on finding the solutions of the Diophantine equation $3^x + p^m n^y = z^2$ where $y = 1, 2$ and $p > 3$ a prime number.

CHAPTER 1

INTRODUCTION

1.1 Introduction to Diophantine Equations

The study of Diophantine equations is the study of integer and rational number solutions to systems of equations or polynomial equations. It has its origins in ancient Babylonian, Egyptian, and Greek writings, making it one of the earliest branches of number theory, if not all of mathematics.

The "Father of Algebra" Diophantus (Heath, 1910) is best known for his book Arithmetica, which deals with solving algebraic equations and number theory. However, only very few pieces of information are known about his life, and there has been significant controversy about the exact years he lived, but it is known that he lived in the 3rd century. Diophantus did mention the definition of a polygonal number from Hypsicles' work, which was written before 150 BCE, therefore we can assume he lived beyond that era (Bashmakova and Silverman, 1997).

One of the great things that Diophantus contributied to mathematics is that he was the first to use symbols in algebra. His contribution to the field was the reason that Diophantine equations were named after him (Heath, 1910).

One of the fascinating aspects of the field is that the problems are often simple to state but extremely difficult to answer, and even when they can be solved, they often necessitate the use of extremely advanced mathematical methods and tools. More importantly, mathematicians frequently must invent and build new ways to address number-theoretical problems, and these approaches become key branches of mathematics with applications in issues other than those for which they were developed.

Many technological, engineering and applied mathematics sectors have benefited from the discovery of the Diophantine Equation. For instance, large values of the argument would not be able to analyze the answer to numerous issues without its assistance (Klykov, 2021). In computer science, in general, and Cryptography, in particular, Diophantine Equations led to the most useful applications where it has been used to determine the level of security based on the level of difficulty of solving a certain class of Diophantine equations (Ding et al., 2018; Klavska, 2017).

Diophantine equations were applied to some problems in chemistry where one can reduce all chemical compounds to a combination of chemical elements, which in turn can help reduce all integers to a product of prime factors in a particular way (Crocker, 1968; Okumura, 2015).

1.2 Literature review

The Diophantine equation $a^x + p^y = z^2$ where $a = 2$ and p is prime is one of the Diophantine equations families that were studied widely by mathematicians. Many fields of mathematics can benefit from Diophantine equations, such as the high-accuracy computation of prime logarithms (Brenner and Foster, 1982). For various primes, some of the equations of the type $a^x + p^y = z^2$ have been entirely solved. In 2007, Acu showed that the only two non-negative integer solutions where $p = 5$ are $(x, y, z) = (3, 0, 3)$ and $(2, 1, 3)$ (Acu, 2007) . Later in 2011, Suvarnamani proved that there is no non-negative integer solution (x, y, z) for the case $p = 7, 11$ when x is even (Suvarnamani et al., 2011).

After Catalan's conjecture was proved, it played a main part in studying several equations of the form $a^x + p^y = z^2$. In 2018, Rabago, using Mihailescu's theorem, proved that the two Diophantine equations $4^x - 7^y = 3z^2$ and $4^x - 19^y = 3z^2$ have only two solutions $(x, y, z) = (0, 0, 0)$ and $(1, 0, 1)$, then stated a generalization for these two equations by proving that the Diophantine equation $4^x - p^y = 3z^2$ has only the two solutions $(0, 0, 0)$ and $(1, 0, 1)$ (Rabago, 2018). The method Rabago's used was similar to what Peker and Cenberci did in 2012, where they gave the solutions for the Diophantine equation $(4^n)^x + p^y = z^2$ (Peker and Cenberci, 2012).

Between the years 2012-2014, Sroysang studied the Diophantine equation $5^x + p^y = z^2$ for the cases where $p = 7, 23, 63$ (Sroysang, 2013c); (Sroysang, 2013b); (Sroysang, 2014c), and the Diophantine equation $3^x + p^y = z^2$ for the cases where $p = 17, 45, 85$ (Sroysang, 2014a); (Sroysang, 2014b); (Sroysang, 2013a). Sroysang work involved the use of Mihailescu's theorem in all the cases.

Recently, Sugandha *et al.* used the theory of congruence to prove that $3^x + 5^y = z^2$ has only one non-negative integer solution $(x, y, z) = (1, 0, 2)$ (Agus et al., 2020). The same result was established earlier in 2012 by Sroysang who used Mihailescu's theorem to determine the solution (Sroysang, 2012).

In 2019, Lipaporn *et al.* studied the Diophantine equation $3^x + p^5 y = z^2$, where x, y and z are non-negative integers and p is a prime number not equal to 2 or 5 (Laipaporn et al., 2019). In the same year, Bakar *et al.* investigated the Diophantine equation

$5^x + p^m n^y = z^2$ to generalize some of Sroysang work by finding the solutions where x, m, n, z are positive integers with $p > 3$ and $y = 1, 2$ (Bakar et al., 2019).

Another work related to Mihailescu's theorem was made by Chotchaisthit who studied the Diophantine Equation $43^n 2^x + 43^y = z^{2m}$ and proved that all non-negative integer solutions are of type $(3, n, 3(43)^2)$ if n is even and $m = 1$ (Chotchaisthit, 2017).

All of the Diophantine Equations mentioned above are special cases of the Diophantine Equation $a^x + b^y = z^2$. Studying these cases would contribute to the finding of a general form of solutions to this family of equations. Inspired by all references mentioned earlier, we will focus on the solvability of some Diophantine Equations of the form $a^x + b^y = z^2$.

Motivated by Rabago's work, we will use Mihailescu's theorem, number theory concepts, and characteristics of congruence to focus on determining the existence of the solution of the Diophantine equations $16^x - 7^y = z^2$, $16^x - p^y = z^2$ and $64^x - p^y = z^2$, after that, we generalize the previous equations where we find the solutions of the Diophantine equation $(4^n)^x - p^y = z^2$. After studing the Diophantine equation $(4^n)^x - p^y = z^2$, we will focus on some Diophantine equations of the type $p^x + p(l)^y = z^2$, where we will determine the solutions of the Diophantine equations $7^x + 11^y = z^2$, $13^x + 17^y = z^2$ and $15^x + 17^y = z^2$ using the theory of congruence and Mihailescu's theorem. Then we focus on finding the solutions for the Diophantine equations $2^x + 257^y = z^2$, $11^n 8^x + 11^y = z^2$ and $3^x + p^m n^y = z^2$.

1.3 Problem statement

In 2004, Catalan's conjecture was proved by Mihailescu, and since then, it was used to solve many Diophantine equations of the type $a^x + b^y = z^2$. Rabago in 2018, by using Mihailescu's theorem showed that the Diophantine equation $4^x - p^y = 3z^2$ has two solutions $(0,0,0)$ and $(1,0,1)$. This, in turn, motivates us to generalize Rabago's work by finding the solutions of the Diophantine equation $(4^n)^x - p^y = z^2$. One year later, Lipaporn *et al.* studied the Diophantine equation $3^x + p^5 y = z^2$, where x, y and z are non-negative integers and p is a prime number not equal to 2 or 5. That, in turn, motivates us to generalize Lipaporn work where we concentrate on finding the solutions of the Diophantine equation $3^x + p^m n^y = z^2$ where x, m, n, z are positive integers with $p > 3$ and $y = 1, 2$. Many other scholars focused on using Mihailescu's theorem to find solutions for special cases of Diophantine equations of the form $a^x + b^y = z^2$. Therefore, we expand the research scope by using various methods to determine the solutions of the Diophantine equations $7^x + 11^y = z^2$, $13^x + 17^y = z^2$, $15^x + 17^y = z^2$, $2^x + 257^y = z^2$ and $11^n 8^x + 11^y = z^2$. Combining various methods and tools to study this specific type of equation can help to gain more understanding of the form of answers given to this family of equations.

1.4 Research objectives

The following are the objectives of this thesis:

1. To obtain all solutions for the Diophantine equations $16^x - 7^y = z^2$, $16^x - p^y = z^2$ and $64^x - p^y = z^2$ and deduce the solutions to the Diophantine equation $(4^n)^x - p^y = z^2$ using Mihailescu's theorem.

2. To determine the existence and produce the solutions (if exist) to the Diophantine equations $7^x+11^y=z^2$, $13^x+17^y=z^2$, $15^x+17^y=z^2$ and $2^x+257^y=z^2$ using theory of congruence and Mihailescu's theorem.

3. To discover all possible solutions to the Diophantine equation $11^n 8^x+11^y=z^2$ using Mathematical induction.

4. To determine the solutions of the Diophantine equation $3^x+p^m n^y=z^2$ using Mihailescu's theorem and by determining bounds on the fundamental solution.

1.5 Thesis outline

The thesis comprises six chapters. Chapter 1 is an introduction to the history and applications of the Diophantine equations, followed by a literature review, then the problem statement and research objectives, ended with the thesis outline. In Chapter 2, we review necessary concepts, definitions, and theorems that are used throughout this thesis. In Chapter 3, the Diophantine equation $16^x-7^y=z^2$ is investigated to prove that it has only two solutions (x,y,z), (the trivial solution) $(0,0,0)$, and $(1,1,3)$, where x,y, and z are non-negative integers, also the Diophantine equations $16^x-p^y=z^2$ and $64^x-p^y=z^2$ were solved, after that, we proved a generalization of the previous equation, where $(4^n)^x-p^y=z^2$ and x,y,z are non-negative integers. Chapter 4 discusses the solvability of the Diophantine equations $7^x+11^y=z^2$, $13^x+17^y=z^2$ and $15^x+17^y=z^2$ using Mihailescu's theorem and the theory of congruence to determine the solutions. In Chapter 5, we study more Diophantine equations of the form $a^x+b^y=z^2$ starting by focusing on determining all possible solutions of the Diophantine equation $2^x+257^y=z^2$ and using the result to investigate three corollaries to show that the Diophantine equations $2^x + 257^y = w^4$ and $8^m + 66049^n = w^4$ have no non-negative integer solutions, and $(m,n,z) = (1,0,3)$ is the only solution for the Diophantine equation $8^m + 66049^n = z^2$, after that we investigate the Diophantine equation $11^n 8^x + 11^y = z^2$. Finally, we concentrate on finding the integral solutions of the Diophantine equation $3^x + p^m n^y = z^2$ where $y = 1,2$ and $p > 3$ a prime number. Chapter 6 contains the conclusions and future work.

CHAPTER 2

PRELIMINARIES

This chapter contains a review of some tools, definitions, lemmas and theorems that will be needed throughout the thesis. Here we focus especially on Catalan's conjecture since it plays a main part of this thesis, also, we give a brief definition and some properties for the theory of congruence, Divisibility and Mathematical Induction.

2.1 Catalan's conjecture

The story of Catalan's conjecture starts in the year 1844 when Catalan (Lebesgue, 1850) proposed the following:

The difference between two perfect powers where we ignore 0 and 1 is always more than 1 unless these powers are equal to $8 = 2^3$ and $9 = 3^2$. In other words,

$$a^x - b^y = 1$$

has the only nontrivial solution: $3^2 - 2^3 = 1$.

In 1850, Lebesgue (Le and Soydan, 2020) proved that the Diophantine Equation $x^m - y^2 = 1$ has no solutions where x, y and m are positive integers with $m > 1$. Fifteen years later, (Ko, 1965) proved that the Equation $x^2 - y^n = 1$ where x, y and n are positive integers and $n > 1$, has the unique solution $x = 3$ and $y = 2$.

(Cassels, 1960) focused on the discovery of important arithmetical properties of

Catalan's equation ($x^p - y^q = 1$) and most subsequent works on Catalan's equation relied heavily on his findings. For more than 150 years, the conjecture has been open, and many mathematicians and researchers have made so much effort to solve it. The conjecture remained unproved until 2004 when Mihailescu managed to prove it (Schoof, 2010). Mihailescu showed that the existence of solutions to Catalan's equation did produce an excess of q-primary cyclotomic units in that case. The previous fact led to a contradiction that proved Catalan's conjecture where Mihailescu stated the following theorem:

Theorem 2.1. *(Mihailescu, 2004): $(3,2,2,3)$ is a unique solution (a,b,x,y) for the Diophantine equation $a^x - b^y = 1$ where a,b,x and y are integers such that* $\min\{a,b,x,y\} > 1$.

After Catalan's conjecture was proved, many researchers relied on it to solve different types of Diophantine Equations, and nowadays, much of the work related to the Diophantine equation $a^x + b^y = c^z$ relies on Catalan's conjecture to study these equations and to determine the solutions.

2.2 Mersenne Primes

When $2^n - 1$ is prime it is said to be a Mersenne prime. In 1664, Mersenne stated that the numbers $2^n - 1$ were prime for:

$$n = 2,3,5,7,13,17,19,31,67,127 \textit{ and } 257.$$

It took three centuries and many mathematical discoveries before the exponents in Mersenne's conjecture had been completely checked. It was determined that he was not completely correct and the correct list is: $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ and 127 (Dickson, 1971). After that, Mersenne primes were studied in depth because of their close connection to perfect numbers. Many properties were discovered during the study of Mersenne primes. One of the most important properties of Mersenne primes is that: if for some positive integer n, $2^n - 1$ is prime, then so is n (Delello, 1986).

2.3 The theory of congruence

Gauss devised an extremely useful concept in number theory that makes a variety of issues involving integer divisibility much easier to solve. This gave birth to the theory of congruences. First, we give a definition and some facts.

Definition 2.1. *(Stein, 2008) Let u, v, r and k be integers and $t \in \mathbb{N}$. Then $u \equiv v \ (\ mod\ t)$ if $t \mid (u - v)$ and $u \not\equiv v(\ mod\ t)$ if $t \nmid (u - v)$.*

Here, are some facts from the definition of Congruence (Crilly, 1978):

- If $u \equiv v\ (mod\ t)$, then $v \equiv u\ (mod\ t)$.
- If $u \equiv v\ (mod\ t)$ and $v \equiv r\ (mod\ t)$, then $u \equiv r\ (mod\ t)$.
- If $u \equiv v\ (mod\ t)$ and $r \equiv k\ (mod\ t)$, then $ur \equiv vk\ (mod\ t)$.
- If $u \equiv v\ (mod\ t)$ and $r \equiv k\ (mod\ t)$, then $u \pm r \equiv v \pm k\ (mod\ t)$.
- If $u \equiv v\ (mod\ t)$, then $u^r \equiv v^r\ (mod\ t)$.

The following are some other facts from the Congruence definition that will be used in this thesis:

- If n is a perfect square, then $n \equiv 1 \ (\ mod\ 4)$ when n is odd, and $n \equiv 0 \ (\ mod\ 4)$ when n is even.

- If n is a perfect square, then $n \equiv 0 \ (\ mod\ 3)$ when n is divisible by 3, and $n \equiv 1 \ (\ mod\ 3)$ when n is not divisible by 3.

- $17^n \equiv 1 \ (\ mod\ 3)$ for every even integer n.

To check the this property, one can show the following:

$$17^1 \equiv 2 \ (\ mod\ 3),$$
$$17^2 \equiv 1 \ (\ mod\ 3),$$
$$17^3 \equiv 2 \ (\ mod\ 3), ...$$

It seems that if n is odd, then $17^n \equiv 2 \ (\ mod\ 3)$, and if n is even, then $17^n \equiv 1 \ (\ mod\ 3)$. This pattern will keep repeating, because in the case where x is even, we have $17^2 \equiv 1 \ (\ mod\ 3)$, and so increasing the exponent n by 2 will never change the remainder $(\ mod\ 3)$ since:

$$17^2 \equiv 1 \ (\ mod\ 3),$$
$$17^1 \cdot 17^1 \equiv 1 \cdot 1 \ (\ mod\ 3).$$

Therefore, 17^n is congruent to $1 \ (\ mod\ 3)$ when n is even.

- $15^n \equiv 0 \ (\ mod\ 3)$ for every integer n.

By using the same method as in the previous property, one can see that:

$$15^1 \cdot 15^1 \equiv 0 \cdot 0 \ (\ mod\ 3),$$

$$15^2 \equiv 0 \ (\ mod\ 3).$$

One can use the same technique, through induction, to show that the powers of 15 are congruent to 0 mod 3 since we can continue multiplying our resulting equation by the initial equation $15^1 \equiv 0 \ (\ mod\ 3)$. Which means that all powers of 15, when divided by 3, give us a remainder of 0.

The same technique applied earlier can be used to show the next two properties.

- $13^n \equiv 1 \ (\ mod\ 4)$ for every integer n.

- $15^n \equiv 1 \ (\ mod\ 4)$ for every integer n.

2.4 Divisibility

One of the most essential concepts in number theory is divisibility. A precise definition of what it means for a number to be divisible by another number is essential for defining other number-theoretic concepts such as that of prime numbers.

Definition 2.2. *(Fine and Rosenberger, 2016) Let $u, v, r \in \mathbb{Z}$, with $u \neq 0$. We say (u divides v) if there exists $t \in \mathbb{Z}$ such that $v = tu$.*

Here are some useful properties of divisibility (Fine and Rosenberger, 2016):

- If $u \mid v$ and $v \mid r$, then $u \mid r$
- If $r \mid u$ and $r \mid v$, then $r \mid u+v$ and $r \mid u-v$
- If $r \mid u$ and $r \mid v$, then, for any $x, y \in \mathbb{Z}$, $r \mid ux+vy$.

2.5 Mathematical Induction

Pascal is credited with being the first to express the principle of induction explicitly (Coughlin and Kerwin, 1985) which have been used later by Fermat who made good use of it in a related technique known as indirect proof by infinite descent (Bussey, 1918).

Definition 2.3. *(Andreescu et al., 2010) Let $(P(n))_{n\geq 0}$ be a sequence of propositions. Mathematical induction assists us in proving that $P(n)$ is true for all $n \geq n_0$, where n_0 is a given non-negative integer.*

Theorem 2.2. *(Kwong, 2015) Let $P(n)$ be a proposition about n. Let $a \in \mathbb{N}$. Suppose that:*

(a) $P(a)$ is true,

(b) for all $n \geq a$, $p(n)$ is true $\Rightarrow p(n+1)$ is also true.

Then $p(n)$ is true for all $n \geq a$.

In general, Mathematical Induction is a mathematical proving method, where we show that a propositional function $p(n)$ is true for all integers $n \geq 1$. To show that, we need to follow two steps:

- Verify that $p(1)$ is true.
- Show that if $p(k)$is true for some integer $k \geq 1$, then $p(k+1)$ is also true.

For example, if we want to use Mathematical Induction to prove that $7+14+21+\ldots+7n=\frac{7n(n+1)}{2}$ is true for every positive integer, first, we have to show that it is true when $n=1$. When $n=1$, we get $7(1)=\frac{7(1)((1)+1)}{2}=7$.

Second, we assume that $n=k$ such that $7+14+21+\ldots+7k=\frac{7k(k+1)}{2}$ is true when $k\geq 1$. Then we have to show that it is true when $n=k+1$ such that $7+14+21+\ldots+7(k+1)=\frac{7(k+1)((k+1)+1)}{2}$ is true when $k\geq 1$.

$$7+14+21+\ldots+7(k+1)=7+14+21+\ldots+7k+7(k+1)$$

$$=\frac{7k(k+1)}{2}+7(k+1)$$

$$=\frac{7k(k+1)}{2}+\frac{14(k+1)}{2}=\frac{7k(k+1)+14(k+1)}{2}$$

$$=\frac{7(k+1)[k+2]}{2}$$

$$=\frac{7(k+1)((k+1)+1)}{2}.$$

By induction, we showed that $7+14+21+\ldots+7n=\frac{7n(n+1)}{2}$ is true for every positive integer.

2.6 Fundamental Solution

Here, we show the definition of a fundamental solution along with a theorem that will be used in chapter 5.

Definition 2.4. *(Mollin, 1997) If $\alpha_j=x_j+y_j\sqrt{D}$ for $j=1,2$ are primitive solutions of the equation $x^2-Dy^2=n$, then they are said to be in the same class provided that* *there is a solution $\beta = u + v\sqrt{D}$ of the equation $x^2 - Dy^2 = 1$ such that $\alpha_1\beta = \alpha_2$. If α_1 and $\alpha_1^{'} = x_1 - y_1\sqrt{D}$ are in the same class, then the class is called ambiguous. In a given class, let $\alpha_0 = x_0 + y_0\sqrt{D}$ be a primitive solution with least possible positive y_0. If the class is ambiguous, then we require that $x_0 \geq 0$. Also, $\mid x_0 \mid$ is the least possible value for any x with $x + y\sqrt{D}$ in its class, and so α_0 is uniquely determined. We call α_0 the fundamental solution in its class.*

Theorem 2.3. *(Sica, 2010) The bound for the fundamental solution (u, v) for the equation $u^2 - Dv^2 = N$ is*

$$0 \leq v \leq \frac{y_1}{\sqrt{2(x_1+1)}}\sqrt{N},$$

$$0 \leq \mid u \mid \leq \sqrt{\frac{1}{2}(x_1+1)N},$$

where N is positive integer with (x_1, y_1) is the fundamental solution of equation $x^2 - Dy^2 = 1$ and D is natural number which is not a perfect square.

2.7 Previous Results

The following are some lemmas that will be used in this study.

Lemma 2.1. *(Sroysang, 2013d) The Diophantine equation $7^x + 1 = z^2$ has no non-negative integer solution where x and z are non-negative integers.*

Lemma 2.2. *(Peker and Cenberci, 2012) $(7, 1, 129)$ is a unique solution (k, y, z) for the Diophantine equation $4^k + 257^y = z^2$, where k, y and z are non-negative integers.*

Lemma 2.3. *(Ivorra, 2003) The Diophantine equation $2^x + 257^y = z^2$ has no solution where x, y and z are non-negative integers with $x \geq 2$ and $y \geq 3$.*

Lemma 2.4. *(Yu and Li, 2014) The Diophantine equation* $2^x + b^y = c^z$ *admits a solution for* $x > 1$, $y = 1$ *and* $2^x < b^{\frac{50}{13}}$.

Lemma 2.5. *(Qi and Li, 2015) If* $p \equiv \mp 3 \pmod 8$, *then the Diophantine equation* $8^x + p^y = z^2$ *has no positive integer solutions.*

In the next chapter, we will focus on some Diophantine equations of the form $a^x - b^y = z^2$, namely $16^x - 7^y = z^2$, also the Diophantine equations $16^x - p^y = z^2$ and $64^x - p^y = z^2$ will be investigated. In addition, we will determine the solutions to the Diophantine equation $(4^n)^x - p^y = z^2$.

CHAPTER 3

ON THE DIOPHANTINE EQUATION $(4^n)^x - p^y = z^2$

In this chapter, the Diophantine equation $(4^n)^x - p^y = z^2$ where p is an odd prime, $n \in Z^+$ and x, y, z are non-negative integers, will be investigated to show that the solutions are given by

$$(x,y,z,p) = (k,1,2^{nk}-1,2^{nk+1}-1) \text{ or } (x,y,z,p) = (0,0,0,p).$$

We will go through some equations that will prepare and structure our way to reach the main theorem. We will start by focusing on the Diophantine equation $16^x - 7^y = z^2$ to find all the possible solutions.

3.1 The Diophantine equation $16^x - 7^y = z^2$

Theorem 3.1. *The Diophantine equation*

$$16^x - 7^y = z^2, \tag{3.1}$$

has only two solutions (x,y,z)*, (the trivial solution)* $(0,0,0)$*, and* $(1,1,3)$.

Proof: Evidently, the case when $z = 0$ will give us $(x,y,z) = (0,0,0)$. For $z > 0$, one can consider the cases below.

Case 1. $x = 0$. This case is trivial.

Case 2. $y = 0$. If $y = 0$, then we have $(2^x)^4 - z^2 = 1$ which is impossible according to Mihailescu's theorem.

Case 3. $x, y > 0$. For this case we have $((2^x)^4 - z^2) = ((2^x)^2 + z)((2^x)^2 - z) = 7^y$. It follows that $((2^x)^2 + z) + ((2^x)^2 - z) = 2^{2x+1} = 7^\alpha + 7^\beta$ for some $\alpha < \beta$, where $\alpha + \beta = y$. Hence, $2^{2x+1} = 7^\alpha(7^{\beta-\alpha} + 1)$. Thus, $\alpha = 0$ and $2^{2x+1} - 7^\beta = 1$, which is true when $x = 1$ and $y = 1$ since $\alpha + \beta = y$ and we have $\alpha = 0$ and $\beta = 1$. These give us the value $z = 3$. Therefore, $(1, 1, 3)$ is a solution of $16^x - 7^y = z^2$. Now, if we assume $y > 1$, then we get $2^{2x+1} - 7^\beta = 1$ which has no solution according to Mihailescu's theorem. Therefore, $(0, 0, 0)$ and $(1, 1, 3)$ are the only solutions for the equation $16^x - 7^y = z^2$.

Next, the Diophantine equation $16^x - p^y = z^2$ will be investigated to find all of the non-negative integer solutions.

3.2 The Diophantine equation $16^x - p^y = z^2$

Theorem 3.2. *All non-negative integer solutions of the Diophantine equation*

$$16^x - p^y = z^2, \tag{3.2}$$

are given as the following:

$$(x, y, z, p) = (k, 1, 2^{2k} - 1, 2^{2k+1} - 1) \text{ or } (x, y, z, p) = (0, 0, 0, p)$$

where k, x, y, z are non-negative integers and p is an odd prime.

Proof: One can consider the following cases

Case 1. $x = 0$. In this case, we have $z^2 + p^y = 1$ which implies that $z = 0$, $y = 0$ and p any prime number.

Case 2. $y = 0$. If $y = 0$, then we have $16^x - 1 = z^2$. From Mihailescu's theorem, one can consider the following four subcases:

Subcase 2.1. $x = 0$, we get $1 - z^2 = 1$, hence $(x,z) = (0,0)$.

Subcase 2.2. $x = 1$, we get $16 - z^2 = 1$, hence $z^2 = 15$, which is impossible.

Subcase 2.3. $z = 0$, we get $16^x = 1$, therefore, $(x,z) = (0,0)$.

Subcase 2.4. $z = 1$, we get $16^x - 1 = 1$, hence $16^x = 2$, which is impossible.

One can see that $16^x - z^2 = 1$ has only the solution $(x,y,z) = (0,0,0)$.

Case 3. $x,y > 0$. For this case we have $16^x - p^y = z^2$ which is equivalent to $(2^{2x} + z) + (2^{2x} - z) = p^y$. It follows that $2^{2x+1} = p^{\alpha}(p^{\beta-\alpha} - 1)$ for some integers α and β where $\alpha + \beta = y$. Thus, $\alpha = 0$ and $2^{2x+1} - p^y = 1$ which has no solution when $x,y > 1$. From Mihailescu's theorem, we have four subcases:

Subcase 3.1. $x = 0$, we get $2 - p^y = 1$, hence, $p^y = 1$, therefore, the solution of the equation $16^x - p^y = z^2$ is $(x,y,z,p) = (0,0,0,p)$.

Subcase 3.2. $x = 1$, we get $8 - p^y = 1$, hence $p^y = 7$, therefore, the solution of the equation $16^x - p^y = z^2$ is $(x,y,z,p) = (1,1,3,7)$.

Subcase 3.3. $y = 0$, we get $2^{2x+1} - 1 = 1$, therefore, the solution of the equation $16^x - p^y = z^2$ is $(x, y, z, p) = (0, 0, 0, p)$.

Subcase 3.4. $y = 1$, we get $2^{2x+1} - p = 1$, hence $p = 2^{2x+1} - 1$. One can see that $2^{2x+1} - 1$ is a prime if and only if $2x + 1$ is also a prime, therefore, we get a family of solutions to the equation $16^x - p^y = z^2$ given by $(x, y, z, p) = (k, 1, 2^{2k} - 1, 2^{2k+1} - 1)$.

□

In the following, the Diophantine equation $64^x - p^y = z^2$ will be solved, as a final step of generalizing the results.

3.3 The Diophantine equation $64^x - p^y = z^2$

Theorem 3.3. *For k, x, y, z are non-negative integers and p is an odd prime, the solutions of the Diophantine equation*

$$64^x - p^y = z^2 \tag{3.3}$$

are given by

$$(x, y, z, p) = (k, 1, 2^{3k} - 1, 2^{3k+1} - 1) \text{ or } (x, y, z, p) = (0, 0, 0, p)$$

Proof: We consider the following cases:

Case 1. $x = 0$. In this case, we have $z^2 + p^y = 1$ which implies that $z = 0$, $y = 0$ and p any prime number.

Case 2. $y = 0$. If $y = 0$, then we have $64^x - 1 = z^2$. From Mihailescu's theorem, one can consider the following four subcases:

Subcase 2.1. $x = 0$, we get $1 - z^2 = 1$, hence $(x, z) = (0, 0)$.

Subcase 2.2. $x = 1$, we get $64 - z^2 = 1$, hence $z^2 = 63$, which is impossible.

Subcase 2.3. $z = 0$, we get $64^x = 1$, therefore, $(x, z) = (0, 0)$.

Subcase 2.4. $z = 1$, we get $64^z - 1 = 1$, hence $64^x = 2$, which is impossible.

One can see that $64^x - z^2 = 1$ has only the solution $(x, y, z) = (0, 0, 0)$.

Case 3. $x, y > 0$. For this case we have $64^x - p^y = z^2$ which is equivalent to $(2^{3x} + z) + (2^{3x} - z) = p^y$. It follows that $2^{3x+1} = p^{\alpha}(p^{\beta-\alpha} - 1)$ for some integers α and β where $\alpha + \beta = y$. Thus, $\alpha = 0$ and $2^{3x+1} - p^y = 1$ which has no solution when $x, y > 1$ according to Mihailescu's theorem. For $x, y < 1$, we have four subcases:

Subcase 3.1. $x = 0$, we get $2 - p^y = 1$, hence, $p^y = 1$, therefore, the solution of the equation $64^x - p^y = z^2$ is $(x, y, z, p) = (0, 0, 0, p)$.

Subcase 3.2. $x = 1$, we get $16 - p^y = 1$, hence $p^y = 15$ which is impossible.

Subcase 3.3. $y = 0$, we get $2^{3x+1} - 1 = 1$, therefore, the solution of the equation $64^x - p^y = z^2$ is $(x, y, z, p) = (0, 0, 0, p)$.

Subcase 3.4. $y = 1$, we get $2^{3x+1} - p = 1$, hence $p = 2^{3x+1} - 1$. One can see that $2^{3x+1} - 1$ is a prime if and only if $3x + 1$ is also a prime, therefore, we get a family of solutions to the equation $64^x - p^y = z^2$ given by $(x,y,z,p) = (k,1,2^{3k}-1,2^{3k+1}-1)$.

□

In the next section, we will present the main theorem of this chapter, where the previous equations will be generalized where we focus on finding the solutions to the Diophantine equation $(4^n)^x - p^y = z^2$.

3.4 The Diophantine equation $(4^n)^x - p^y = z^2$

The generalization of the previous Diophantine equations is given in the following theorem.

Theorem 3.4. *The solutions of Diophantine equation*

$$(4^n)^x - p^y = z^2 \tag{3.4}$$

are given by

$$(x,y,z,p) = (k,1,2^{nk}-1,2^{nk+1}-1)$$

where x,y,z are non-negative integers, k is a positive integer, and $2^{nk+1}-1$ *is a prime.*

Proof: To solve this equation we will consider three cases where $y = 0$, $y = 1$, and $y \geq 2$.

For $y = 0$, the equation (3.4) becomes $4^{nx} - 1 = z^2$. If $x > 0$, then we have $-1 \equiv z^2 \pmod 4$, which is impossible, because squares are always $\equiv 0$ or $\equiv 1 \pmod 4$. Therefore $x = 0$ and the equation becomes $0 = z^2$, so $z = 0$. Also p is arbitrary. This is the trivial solution.

The cases $y = 1$ and $y \geq 2$ are similar to each other. We can use some divisibility observations here.

From (3.4) we have

$$p^y = (2^{nx} - z)(2^{nx} + z).$$

The two factors on the right cannot both be divisible by p, because their sum is 2^{nx+1} which is not divisible by p. But they are both powers of p, so the smaller one is $2^{nx} - z = 1$ and the larger one is $2^{nx} + z = p^y$. Solving this system of two equations we obtain

$$p^y = 2^{nx+1} - 1, \tag{3.5}$$

$$z = 2^{nx} - 1.$$

If $y \geq 2$, we have that the equation (3.5) is impossible by Mihailescu's theorem, because both exponents are greater than or equal to 2 and it is not the one permissible case $3^2 - 2^3 = 1$.

If $y = 1$, from (3.5), we have $p = 2^{nx+1} - 1$, thus all combinations of this form are solutions. That is, if k is a positive integer and $2^{nk+1} - 1$ is prime, then

$$(x, y, z, p) = (k, 1, 2^{nk} - 1, 2^{nk+1} - 1)$$

is a solution of (3.4), because we have

$$z^2 = (2^{nk} - 1)^2 = 2^{2nk} - 2^{nk+1} + 1 = (4^n)^k - p^1.$$

This completes the proof of the Main Theorem

3.5 Summary

In this chapter, we showed that the Diophantine equation $16^x - 7^y = z^2$ has only two solutions (x, y, z), (the trivial solution) $(0, 0, 0)$, and $(1, 1, 3)$, where x, y, and z are non-negative integers. Also the Diophantine equations $16^x - p^y = z^2$ and $64^x - p^y = z^2$ have been solved to move to the main part of the chapter where we proved a generalization of the previous results, by investigating the Diophantine equation $(4^n)^x - p^y = z^2$ where x, y, z are non-negative integers. We proved that the solutions are given by

$$(x, y, z, p) = (k, 1, 2^{nk} - 1, 2^{nk+1} - 1) \text{ or } (x, y, z, p) = (0, 0, 0, p).$$

And we noticed that some of the solutions contain parts that similar to Mersenne prime, which is a prime number of the form $2^p - 1$ where p is a prime.