Upper Bounds for the Number of Solutions for the Diophantine Equation $y^2 = px(Ax^2 - C), C \in \{2, \pm 1, \pm 4\}$

Zak Schedler
4927794

Submitted in partial fulfillment
of the requirements for the degree of
Master of Science, Mathematics

Faculty of Mathematics, Brock University
St. Catharines, Ontario

Abstract

A Diophantine equation is an equation of more than one variable where we are looking for strictly integer solutions. The purpose of this paper is to give a new upper bounds for the number of positive solutions for the Diophantine equation $y^2 = px(Ax^2 - C),\ C \in \{2, \pm 1, \pm 4\}$. Where p is an odd prime and A is an integer greater than 1. The case where $C = -2$ is already complete, which we go over in detail here. We look through examples of Diophantine equations starting with linear Diophantine equations. We then look at Pell's equation, $x^2 - Dy^2 = C$ where D and C are natural numbers. We show the continued fraction algorithm and how to use it to solve Pell's equation. We will look at proofs and lemmas surrounding particular cases of the Diophantine equation $y^2 = px(Ax^2 - C)$. Then focus on finding the upper bounds of the equation. Then we conclude by showing the new upper bounds of the Diophantine equation $y^2 = px(Ax^2 - C),\ C \in \{2, \pm 1, \pm 4\}$.

Acknowledgements

I would like to thank my supervisor Omar Kihel for all his help through this paper and my whole mathematics career. His assistance and patience are a large part of how I completed this work. I would also like to thank Rachid Boumahdi for all his help and knowledge while writing this paper.

Contents

Chapter 1

Introduction

A Diophantine equation is a polynomial equation of more than one variable where we are looking for strictly integer solutions. These equations contain integer coefficients and are sometimes extended to rational coefficients. The study of Diophantine equations has many paths to follow when looking at different equations. Many of the equations take the form of easy to say puzzle like analogies such as: When does the sum of two squares equal the difference of two other squares? Throughout the history of these equations most authors take an equation that is known, and change it in some way to see the ways of solving it no longer apply. We will state the simplest of Diophantine equations and then see how we have augmented it over history.

One of the simplest examples of a Diophatine equation is

$$ax + by = 1.$$

Where a and b are relatively prime integers. Linear Diophantine equations are very well understood today. Geometrically, $ax + by = 1$ is a straight line. Of course we know this has an infinite number of solutions (x, y) such that x and y are both integers. This equation was extended to

$$ax + by = c,$$

where c is also an integer but a and b are no longer required to be relatively prime. This has solutions only when $gcd(a, b)$ divides c.

Moving away from linear Diophantine equations, we can continue to change these equations to this, the very well known equation from Pythagorean theorem.

$$a^2 + b^2 = c^2$$

where a, b, and c are all integers. These have interesting solutions called Pythagorean triples. Where all three numbers that form a solution are incremented. One such example is $(a, b, c) = (3, 4, 5)$. Keeping in the form of degree two, there are very interesting equations in quadratic form which we

look at here. We will look into Pell's equation which takes the form

$$x^2 - Dy^2 = 1$$

where D is a positive, non square integer. Lagrange proved that if D is not a perfect square, then Pell's equation has infinitely many solutions in the integers. Pell's equation has an interesting story as to how it got its name. Leonhard Eular made a mistake attributing a solution to John Pell when it was not done by him. We can change parameters on $x^2 - Dy^2 = 1$ from when it is equal to one to when it is equal to $C \in \mathbb{Z}$. It is interesting to note that these solutions have a relationship back to when when the equation is equal to 1.

For solving Pell's equation we can use something called a continued fraction. These can be written as an integer plus a fraction iteratively or they can written similarly to a sequence. We can use them to approximate any real number and are a great tool to use to approximate rational numbers. They can also be used to solve Pell's equation and help yield solutions to numarical examples.

Further generalizations can be seen going into Fermat's Last Theorem which generalizes not on the coefficients but on the powers. Fermat's Last theorem famously says the Diophantine equation

$$a^n + b^n = c^n$$

has no solutions in the integers for a, b, and c being integers. This equation has a very famous story behind it. Fermat wrote this in the margins of his copy of Arithmetica stating that he had a proof in 1637. It was not until 1995 when the full proof was published.

Diophantine equations are not limited to finite terms. The Diophantine equation

$$a = 1(b_1^2) + 2(b_2^2) + 3(b_3^2) + ...$$

is also a type of Diophantine equation. These are not covered at all in this paper but they do exist.

Summarizing what we are going to do in this paper. We present new upper bounds of the number of solutions to $y^2 = px(Ax^2 - C)$, when $C \in \{2, \pm 1, \pm 4\}$, p is an odd prime, and A is an integer greater than one. The goal of this is to classify solutions to know when we have a certain number of solutions. Given p and A after this paper we know how many solutions at most $y^2 = px(Ax^2 - C)$ can have. This is very helpful when trying to find all solutions to a given equation. We do this by using the Legendre symbol and reducing the Diophantine equation modulo 8.

Before we get to that though we review Pell's equation. $x^2 - Dy^2 = \pm 1$ when $D \in \mathbb{N}$. To see when this equation is solvable or not and how many solutions it has. We go over how these solutions relate to each other as well. Then the generalized Pell's equation $x^2 - Dy^2 = C$ where $C \in \mathbb{N}$. During this review we present a Maple program which can solve Pell's equation and find its fundamental solution.

After Pell's equation we look at continued fractions. How to write them using the continued fractions algorithm, and a Maple program is given to produce

a continued fraction for any number. As it turns out we can use continued fractions to solve Pell's equation.

The following two sections are used to go over main results that we used to show new upper bounds of $y^2 = px(Ax^2 - C)$. With proofs that help shape how we proved the new results. These results are important to know because they make our results much easier to prove.

Finally we get into the new results which are soon to be published. Cassels equation came when he tried to solve when the sum of three cubes equals a square. He reduced this problem to solving $y^2 = 3x(x^2 + 2)$. He also provided three solutions. From then, we have generalized this equation and extended it. One of the first generalizations was $y^2 = nx(x^2 + 2)$ where n is a positive integer. This was found to have $3(2^{\omega(n)-1})$ solutions where $\omega(n)$ is the number of distinct prime divisors of n. Naturally it was generalized to if $n = p$ an odd prime which has at most 2 positive solutions. Togbe added another variable $y^2 = px(Ax^2 + 2)$. Li and Yuan looked at when $y^2 = px(Ax^2 - 2)$. Then Wu. et al. considered even more values $y^2 = px(Ax^2 - C)$ where $C \in \{\pm 1, \pm 4\}$ which brings us to the equation we found new bounds for.

Chapter 2

Pell's Equation & Continued Fractions

In this section we are going to summarize what we need in order to prove existence and infiniteness of solutions to $x^2 - Dy^2 = 1$. We will then prove the conditions when $x^2 - Dy^2 = -1$ is solvable. We extend this to when $x^2 - Dy^2 = C$ and go through some examples with a Maple program to solve these equations for us. Finally in this section we look at continued fractions and how they relate to Pell's equation. We include the continued fraction algorithm and use this to solve some Pell equations and provide a Maple program to take a number and write it as a continued fraction using the continued fraction algorithm.

2.1 The Diophantine Equation $x^2 - Dy^2 = 1$

Unless otherwise noted, assume x, y, and D are natural numbers. Consider the ring $\mathbb{Z}[\sqrt{D}]$. This contains elements in the form $a = a_1 + \sqrt{D}a_2$ where a_1 and a_2 are both elements of $\mathbb{Z}$. Similar to the complex field we have $\bar{a} = a_1 - \sqrt{D}a_2$, call $\bar{a}$ the conjugate element of a. This ring is important because if we consider the multiplication of $a\bar{a} = (a_1 + \sqrt{D}a_2)(a_1 - \sqrt{D}a_2) = a_1^2 - Da_2^2$.

Let's give this mapping a name, call it "the norm" and write it like this:

$$N(a) = a\bar{a}.$$

Take a second and consider where the norm takes our element of the ring $\mathbb{Z}[\sqrt{D}]$. We can write that like this $N : \mathbb{Z}[\sqrt{D}] \longrightarrow \mathbb{Z}$. So if we find elements in $\mathbb{Z}[\sqrt{D}]$ whose norm equals 1, then we have found solutions to the Diophantine equation $x^2 - Dy^2 = 1$

Theorem 2.1.1. *There is at least one solution to* $x^2 - Dy^2 = 1$

First we prove this lemma.

Lemma 2.1.2. *If D is any natural number which is not a perfect square, there are an infinite number of natural numbers x and y which satisfy the inequality*

$$|x^2 - Dy^2| < 1 + 2\sqrt{D}.$$

Proof. $\sqrt{D}$ is irrational and we know that

$$|x - \sqrt{D}y| < \frac{1}{y}$$

has an infinite number of solutions.

$$|x + \sqrt{D}y| = |x - y\sqrt{D} + 2\sqrt{D}| < \frac{1}{y} + 2\sqrt{D}.$$

If we factor

$$|x^2 - Dy^2| = |x - \sqrt{D}y||x + \sqrt{D}y| < \frac{1}{y}\big(\frac{1}{y} + 2\sqrt{D}\big) < 1 + 2\sqrt{D}.$$

This means we have an infinity of integral solutions x and y which satisfies $|x^2 - Dy^2| < 1 + 2\sqrt{D}$. Which completes the lemma.

□

On to the proof of 2.1.1

Proof. From 2.1.2 this implies that there exists at least one integer k different from zero, such that

$$x^2 - Dy^2 = k$$

for an infinite number of pairs of integers (x, y). In the set of pairs there must be be at least two pairs (x_1, y_1) and (x_2, y_2) which satisfy this condition:

$$x_1 \equiv x_2 \ (mod\ |k|)$$

and

$$y_1 \equiv y_2 \ (mod\ |k|).$$

If we consider the remainders modulo $|k|$ of the four numbers x_1, x_2, y_1, y_2 we can combine them in k^4 ways. So we have

$$x_1^2 - Dy_1^2 = x_2^2 - Dy_2^2 = k.$$

Following this we have

$$(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = x_1x_2 - y_1y_2D + \sqrt{D}(x_1y_2 - x_2y_1)$$

using the 2 equivalence relations and that both equations equal k. We have

$$x_1x_2 - y_1y_2D \equiv x_1^2 - y_1^2D \equiv 0(mod\ |k|)$$

and

$$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0(mod\ |k|).$$

Therefore

$$x_1x_2 - y_1y_2D = ku$$

and

$$x_1y_2 - x_2y_1 = kv.$$

Where $u, v \in \mathbb{Z}$ so we can write these two equations:

$$(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = k(u + \sqrt{D}v)$$

and

$$(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D}) = k(u - \sqrt{D}v).$$

Multiply these last two equations together to get

$$(x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = k^2(u^2 - Dv^2).$$

Remember that each of the left hand terms of this equation $= k$ so

$$k^2 = k^2(u^2 - Dv^2).$$

Dividing by k^2 we get

$$u^2 - Dv^2 = 1.$$

This proves our theorem.

□

After this, we know there is at least one solution to this equation. If we can prove that the norm operation is closed under multiplication then that will prove that multiplications of two solutions is also a solution. It would also prove that n multiplications of that solution is a solution, giving us an infinite number of solutions.

Theorem 2.1.3. *$N : \mathbb{Z}[\sqrt{D}] \longrightarrow \mathbb{Z}$ defined as $N(a) = a\bar{a}\ \ \forall a \in \mathbb{Z}[\sqrt{D}]$ is closed under multiplication.*

Proof. Let $a, b \in \mathbb{Z}[\sqrt{D}]$ such that $a = a_1 + a_2\sqrt{D}$ and $b = b_1 + b_2\sqrt{D}$.

1. $N(e) = N(1 + 0\sqrt{D}) = (1 + 0\sqrt{D})(1 - 0\sqrt{D}) = 1$
2. $N(ab) = N((a_1 + \sqrt{D}a_2)(b_1 + \sqrt{D}b_2))$
   $= N((a_1b_1 + a_2b_2D) + \sqrt{D}(a_1b_2 + a_2b_1))$
   $= (a_1b_1 + a_2b_2D)^2 - D(a_1b_2 + a_2b_1)^2$
   $= (a_1b_1)^2 + 2a_1b_1a_2b_2D + (a_2b_2D)^2 - D((a_1b_2)^2 + 2a_1b_2a_2b_1 + (a_2b_1)^2)$
   $= (a_1b_1)^2 + (a_2b_2D)^2 - (a_1b_2)^2D - (a_2b_1)^2D$

   $N(a)N(b) = N(a_1 + \sqrt{D}a_2)N(b_1 + \sqrt{D}b_2)$
   $= (a_1^2 - Da_2^2)(b_1^2 - Db_2^2)$
   $= (a_1b_1)^2 + (a_2b_2D)^2 - (a_1b_2)^2D - (a_2b_1)D$
   Therefore $N(ab) = N(a)N(b)$ and the claim is proven.

The means that N is closed under multiplication so if we have one solution we can multiply it by it self and find an infinite number of solutions! $\square$

Definition 2.1.4. If we consider all solutions to $x^2 - Dy^2 = 1$ then we call the solution with least positive x_0 and y_0 the fundamental solution of $x^2 - Dy^2 = 1$. Write it like this

$$x_0 + y_0\sqrt{D}.$$

Example 2.1.5. Solve $x^2 - 6y^2 = 1$
Rearrange this to see $x^2 = 1 + 6y^2$. Try $y = 1$.
$x^2 = 1+6(1)^2 = 7$ So we know $y = 1$ is not a solution because 7 is not a square! Lets try $y = 2$.
$x^2 = 1 + 6(2)^2 = 25$ so if we only consider positive solutions right now the fundamental solution is $(x, y) = (5, 2) = 5 + 2\sqrt{6}$.
From this solution we can find another one. Let's calculate $(5 + 2\sqrt{6})^2$ and see if it's a solution.
$(5 + 2\sqrt{6})^2 = 25 + 20\sqrt{6} + 24 = 49 + 20\sqrt{6}$
$(49)^2 - 6(20)^2 = 1$

Theorem 2.1.6. *If $x_0 + y_0\sqrt{D}$ is the fundamental solution to $x^2 - Dy^2 = 1$ then any solution of this equation is given by*

$$x_n + y_n\sqrt{D} = (x_0 + y_0\sqrt{D})^n$$

where x_n and y_n are given by:

$$\begin{cases} x_n = x_0^n + \sum_{k=1}^{n} \binom{n}{2k} x_0^{n-2k} y_0^{2k} D^k \\ y_n = \sum_{k=1}^{n} \binom{n}{2k-1} x_0^{n-2k+1} y_0^{2k-1} D^{k-1} \end{cases}$$

2.2 The Diophantine Equation $x^2 - Dy^2 = -1$

This equation, unlike the positive version, is not always solvable. It is only solvable for certain values of D.

Theorem 2.2.1. *Two necessary conditions of the solvability of $x^2 - Dy^2 = -1$ are:*

1. *That all odd prime factors of D be of the form $4n + 1$*
2. *If D is even, then it must not be divisible by 4*

Proof. 1. Assume P is an odd prime factor that divides D.
$x^2 - Dy^2 = -1$ take this equation $(mod\ P)$ on both sides.
$x^2 \equiv -1\ (mod\ P)$
Consider the Legendre Symbol:
$\left(\frac{-1}{P}\right) = 1 \Longrightarrow (-1)^{\frac{p-1}{2}}$
$\frac{p-1}{2} = 2n$ rearrange this to see that $p = 4n + 1$

2. Assume D is divisible by 4.
   $x^2 - Dy^2 = -1$ take this equation $(mod\ 4)$ on both sides.
   $x^2 = -1\ (mod\ 4)$ this has no solutions!

□

Definition 2.2.2. Similar to to the positive case, if we consider all solutions to $x^2 - Dy^2 = -1$, then we call the solution with the least positive x_0 and y_0 the fundamental solution to $x^2 - Dy^2 = -1$. Again, write it like this

$$x_0 + y_0\sqrt{D}.$$

Theorem 2.2.3. *If $x^2 - Dy^2 = -1$ is solvable with $x_0 + y_0\sqrt{D}$ being the fundamental solution, then $(x_0 + y_0\sqrt{D})^2$ is the fundamental solution to $x^2 - Dy^2 = 1$.*
If we consider the solutions $(x_0 + y_0\sqrt{D})^n$ where $n \in \mathbb{N}$ then if n is even, $(x_0 + y_0\sqrt{D})^n$ is a solution to $x^2 - Dy^2 = 1$. If n is odd then $(x_0 + y_0\sqrt{D})^n$ is a solution to $x^2 - Dy^2 = -1$. These are the only solutions we have

Example 2.2.4. Consider $x^2 - 34y^2 = -1$
Let's check the necessary conditions $D = 34 = 2(17)$

1. $17 = 4(4) + 1$ so the first condition is satisfied.
2. $34 \equiv 2\ (mod\ 4)$ So D is not a divisor of 4. Both necessary conditions are satisfied.

Consider $x^2 - 34y^2 = 1$ We know this has a solution so lets find it.
$x^2 = 1 + 34y^2$
Let $y = 1$ then $x^2 = 35$ which is not a square.
Let $y = 2$ then $x^2 = 141$ which is not a square.
...
Let $y = 6$ then $x^2 = 1225 = 35^2$. So $35 + \sqrt{34}6$ is the fundamental solution of $x^2 - 34y^2 = 1$. By 2.1.6 we know:
$(x_0 + \sqrt{34}y_0)^2 = 35 + \sqrt{34}(6)$
Where $x_0 + \sqrt{34}y_0$ is the fundamental solution of $x^2 - Dy^2 = -1$
Expanding the left side of the equation:
$x_0^2 + 34y_0^2 + 2x_0y_0\sqrt{34} = 35 + \sqrt{34}(6)$ This can only be true if:
$x_0^2 + 34y_0^2 = 35$ and $2x_0y_0 = 6$
Starting with the second equation $x_0y_0 = 3$ leading to 2 possibilities: $x_0 = 1$ and $y_0 = 3$ or vice-versa:

$$x_0^2 + 34y_0^2 = 35,$$
$$1^2 + 34(3^2) \neq 35,$$
$$3^2 + 34(1^2) \neq 35,$$

Therefore $x^2 - 34y^2 = -1$ has no solutions in the integers.

2.3 The Diophantine Equation $x^2 - Dy^2 = C$

Theorem 2.3.1. *If $x^2 - Dy^2 = C$ is solvable and $x_0 + y_0\sqrt{D}$ is a solution to $x^2 - Dy^2 = C$ with $u_0 + v_0\sqrt{D}$ being a solution to $x^2 - Dy^2 = 1$ then*

$$(x_0 + y_0\sqrt{D})(u_0 + v_0\sqrt{D})$$

is a solution to $x^2 - Dy^2 = C$ too.

Proof. Let $a = x_0 + y_0\sqrt{D}$ and $b = u_0 + v_0\sqrt{D}$ recall the function N is a homomorphism so

$$N(ab) = N(a)N(b)$$

with $N(a) = C$ and $N(b) = 1$ so

$$N(ab) = C(1) = C.$$

Therefore ab is a solution to $x^2 - Dy^2 = C$. □

Definition 2.3.2. Two solutions $x_0 + y_0\sqrt{D}$ and $x_1 + y_1\sqrt{D}$ are associated solutions if there exists a solution $u_0 + v_0\sqrt{D}$ to $x^2 - Dy^2 = 1$ such that:

$$(x_0 + y_0\sqrt{D})(u_0 + v_0\sqrt{D}) = (x_1 + y_1\sqrt{D}).$$

2.4 Maple Program to Solve $x^2 - Dy^2 = C$

```
1  Dee := 804;
2  Cee := 1;
3  y := 1;
4  x := sqrt(Dee*y^2+Cee);
5  if not (type(x, integer)) then
6      while true do
7          y := y+1;
8          x := sqrt(Dee*y^2+Cee);
9
10         if type(x, integer) then
11             break ;
12         end if
13     end do
14 end if
15
16 #This is an output line
17 print(cat("Fundamental Solution is (x, y) = (", x, " , ", y, ")"));
18 print(cat("x^2 -", Dee, "y^2 = ", x, "^2 - ", Dee, "(", y, "^2", ") = ",
19     -Dee*y^2+x^2));
20
21 #This is calculating the n'th solution
22 if `or`(Cee = 1, Cee = -1) then
23     n := 3;
```

```
    x_n := x^n+sum(binomial(n, 2*k)*x^(n-2*k)*y^(2*k)*Dee^k, k=1..n);
    y_n := sum(binomial(n, 2*k-1)*x^(n-2*k+1)*y^(2*k-1)*Dee^(k-1),
        k=1..n);
    print(cat("x_", n, " = ", x_n));
    print(cat("y_", n, " = ", y_n));
    print(cat("x_", n, "^2", " - ", Dee, "y_", n, "^2 = ",
        -Dee*y_n^2+x_n^2))
end if
```

The output to this example is:

```
"Fundamental Solution is (x, y) = (515095 , 18166)"
"x^2 -804y^2 = 515095^2 - 804(18166^2) = 1"
"x_3 = 546665912276384215"
"y_3 = 19279420228174434"
"x_3^2 - 804y_3^2 = 1"
```

2.5 Continued Fractions & How They Relate to Pell's Equation

Definition 2.5.1. Let $\alpha \in \mathbb{R}$. The representation below is called a continued fraction.

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

where $a_n \in \mathbb{N}^*$. If the a_n's are finite we call it a finite continued fraction. Similarly for the infinite case.

Using Continued fractions is a way to approximate real numbers such as $\sqrt{2}$ by using rational numbers.

Example 2.5.2.

Let $\alpha = \frac{13}{6}$

$$\alpha = \frac{12}{6} + \frac{1}{6}$$
$$\alpha = 2 + \frac{1}{6}$$

Example 2.5.3. Let $\beta = \dfrac{122}{57}$ Do the same thing as 2.5.2.

$$\beta = 2 + \frac{8}{57}$$

Let's flip the second term to get the 57 on top.

$$\beta = 2 + \cfrac{1}{\cfrac{57}{8}}$$

Let's treat the $\frac{57}{8}$ as it's own term, and break it up like we did in the previous step.

$$\beta = 2 + \cfrac{1}{7 + \cfrac{1}{8}}$$

Definition 2.5.4. As you can see, carrying continued fractions around can be a cumbersome task. We adopt a condensed notation of writing only the a_n's in an array. Take 2.5.3 for example:

$$\beta = 2 + \cfrac{1}{7 + \cfrac{1}{8}} = [2, 7, 8].$$

2.6 The Continued Fraction Algorithm

This algorithm will allow us to write any number, $x \in \mathbb{R}$, as a continued fraction.
Write

$$x = a_0 + t_0$$

such that $a_0 \in \mathbb{Z}$, and $t_0 \in [0, 1]$. If $t_0 \neq 0$ then write

$$\frac{1}{t_0} = a_1 + t_1$$

$a_1 \in \mathbb{N}$ and $t_1 \in [0, 1]$ and solve this for t_0.

$$t_0 = \frac{1}{a_1 + t_1}$$

and continue this as long as $t_n \neq 0$.

$$\frac{1}{t_n} = a_{n+1} + t_{n+1}$$

with $a_{n+1} \in \mathbb{N}$ and $t_{n+1} \in [0, 1]$

We can associate a real number x to a sequence of integers $a_0,\ a_1,\ ...$

Example 2.6.1. Write α as a continued fraction.

$$\alpha = 1 + \sqrt{2}$$

$$\alpha = 2 + (1 + \sqrt{2} - 2) = 2 + (\sqrt{2} - 1).$$

Consider the 2 before the bracket to be a_0 and call $t_0 = \sqrt{2} - 1$. What is $\frac{1}{t_0}$?

$$\frac{1}{t_0} = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{(\sqrt{2} + 1)(\sqrt{2} - 1)} = \sqrt{2} + 1.$$

So we have

$$\alpha = 2 + \frac{1}{1+\sqrt{2}} = 2 + \frac{1}{\alpha}.$$

Continuing the pattern we can see

$$\alpha = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

Rewriting this

$$\alpha = [2, 2, 2, 2, 2, 2, ...].$$

Theorem 2.6.2. *$\alpha \in \mathbb{Q} \Leftrightarrow$ its continued fraction is finite.*

Proof. Let $\alpha \in \mathbb{Q} \Rightarrow \alpha = \frac{a}{b}$, $b > 0$.
Using Euclid's algorithm we can see

$$a = ba_0 + r_1,$$

$$b = r_1 a_1 + r_2,$$

$$\cdots$$

$$r_{n-2} = r_{n-1}a_{n-1} + r_n,$$

$$r_{n-1} = r_n a_n + 0.$$

We know that $a_i > 0,\ \forall i > 0$.
Rewrite this as:

$$\frac{x}{y} = a_0 + \frac{r_1}{y} = a_0 + \frac{1}{\frac{y}{r_1}}$$

$$\frac{y}{r_1} = a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}}$$

$$\cdots$$

$$\frac{r_{n-1}}{r_n} = a_n \Rightarrow \frac{x}{y} = [a_0, a_1, ..., a_n].$$

□

Definition 2.6.3. A continued fraction $\alpha = [a_0, a_1, ..., a_n, ...]$ is called periodic if there exists $h \in \mathbb{N}$ and for all sufficiently large n we have:

$$a_n = a_{n+h}.$$

We call h the period and write the repeating part of the continued fraction as

$$[a_0, a_1, ..., \overline{a_n, ..., a_{n+h}}].$$

In 2.6.1 we can write $\alpha = [2, 2, 2, 2, 2, ...]$ as

$$\alpha = [\overline{2}].$$

Definition 2.6.4. Construct the following two sequences:

$$p_{-1} = 1,\ p_0 = a_0,\ p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1, \cdots,$$

$$p_n = a_n p_{n-1} + p_{n-2}.$$

$$q_{-1} = 0,\ q_0 = 1,\ q_1 = a_1 q_0 + q_{-1} = a_1, \cdots,$$

$$q_n = a_n q_{n-1} + q_{n-2}.$$

Theorem 2.6.5.

$$[a_0, a_1, \cdots, a_n] = \frac{p_n}{q_n}$$

Proof. Proof by induction.

Base Case

$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1} = \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}} = \frac{p_1}{q_1}$$

Therefore base case holds.

Induction Hypothesis

Assume $[a_0, a_1, \cdots, a_n] = \frac{p_n}{q_n}$ for any arbitrary $n \in \mathbb{N}$

Prove $n+1$

$$[a_0, a_1, \cdots, a_n, a_{n+1}] = \left[a_0, a_1, \cdots, a_n + \frac{1}{a_{n+1}}\right]$$

by induction hypothesis we have

$$= \frac{\left(a_n + \frac{1}{a_{n+1}}\right)p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right)q_{n-1} + q_{n-2}}$$

Multiplying this quotient by $1 = \frac{a_{n+1}}{a_{n+1}}$ leaves us with

$$= \frac{a_{n+1}}{a_{n+1}}\left(\frac{\left(a_n + \frac{1}{a_{n+1}}\right)p_{n-1} + p_{n_2}}{\left(a_n + \frac{1}{a_{n+1}}\right)q_{n-1} + q_{n-2}}\right)$$

$$= \frac{(a_{n+1}a_n + 1)p_{n-1} + a_{n+1}p_{n-2}}{(a_{n+1}a_n + 1)q_{n-1} + a_{n+1}q_{n-2}}$$

expand this and collect the a_{n+1} terms

$$= \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}}$$

$$= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}$$

Completing the proof. □

Theorem 2.6.6. *An infinite integral continued fraction is periodic $\Leftrightarrow$ it represents a quadratic irrational.*

Theorem 2.6.7. *Consider the equation $x^2 - Dy^2 = 1$ and let m be the period of $\sqrt{D}$.*

1. *If m is even then $p_{m-1} + q_{m-1}\sqrt{D}$ is the fundamental solution of $x^2 - Dy^2 = 1$.*
2. *If m is odd then $p_{2m-1} + q_{2m-1}\sqrt{D}$ is the fundamental solution of $x^2 - Dy^2 = 1$.*

Example 2.6.8. Solve the equation $x^2 - 7y^2 = 1$.
Using our continued fractions algorithm we can see that:

$$\sqrt{7} = [2, \overline{1, 1, 1, 4}].$$

So $m = 4$, and therefore even. We are going to use the first part of 2.6.7 to calculate the answer.

We need to calculate $p_{(4-1)} = p_3$ and $q_{(4-1)} = q_3$. Lets do p_3 first:
$p_{-1} = 1$.
$p_0 = a_0 = 2$.
$p_1 = a_1(p_0) + p_{-1} = 1(2) + 1 = 3$.
$p_2 = a_2(p_1) + p_0 = 1(3) + 2 = 5$.
$p_3 = 1(5) + 3 = 8$.
On to q_3:
$q_{-1} = 0$.
$q_0 = 1$.
$q_1 = a_1 q_0 + q_{-1} = 1(1) + 0 = 1$.
$q_2 = a_2 q_1 + q_0 = 1(1) + 1 = 2$.
$q_3 = a_3 q_2 + q_1 = 1(2) + 1 = 3$.
Therefore $(8, 3)$ is the fundamental solution to $x^2 - 7y^2 = 1$. Let's check it!

$$8^2 - 7(3^2) = 64 - 7(9) = 64 - 63 = 1.$$

2.7 Maple Program to Write a Continued Fraction

```
a := sqrt(13);
a_0 := floor(a):
afrac := [a_0]:
t_0 := a-a_0:
while t_0 != 0 do
    temp := 1/t_0;
    a_1 := floor(temp);
    t_1 := temp-a_1;
```

```
    t_0 := t_1;
    afrac := [op(afrac), a_1];
    if not (type(a_1, 'integer')) then
        lengthOfList := numelems(afrac);
        afrac := subsop(lengthOfList = NULL, afrac);
        break
    end if
end do;
afrac;

with(numtheory):
cfrac(a):
```

Output of this program would be:

```
[3,1,1,1,1,6,1,1,1,1,6,1,1,1,1]
```

If one would like to check the solution, change the `cfrac(a):` to `cfrac(a);` This will show Maple's calculation of an extended continued fraction on `a`

Chapter 3

Some Cases of the Diophantine Equation $y^2 = nx(Ax^2 \pm C)$

In this section we go over many proofs and mention some very important lemmas needed to prove not only these proofs but we also use them in the future sections. This are proofs are the ground work for the original material in Chapter 5. We get to see the proofs and techniques used before we need to use it on some harder examples.

Ljunggren proved the following result in [10].

Lemma 3.0.1. *If a and b are odd positive integers, then the Diophantine equation $aX^2 - bY^4 = 2$ has at most two positive integer solutions (X, Y).*

This was improved by Luca and Walsh

Lemma 3.0.2. *If (a_1, b_1) is the minimal positive solution to the Diophantine equation $aX^2 - bY^2 = 2$ and $\alpha^k = \frac{a_k\sqrt{a}+b_k\sqrt{b}}{\sqrt{2}}$ where a_k and b_k are positive integers, then:*

1. *If b_1 is not a square then the Diophantine equation $aX^2 - bY^4 = 2$ has no solutions.*
2. *If b_1 is a square and b_3 is not a square then $(X, Y) = (a_1, \sqrt{b_1})$ is the only solution of the Diophantine $aX^2 - bY^4 = 2$.*
3. *If b_1 and b_3 are both squares then $(X, Y) = (a_1, \sqrt{b_1})$ and $(a_3, \sqrt{b_3})$ are the only solutions of the Diophantine equation $aX^2 - bY^4 = 2$.*

Ljunggren proved the following result in [10].

Lemma 3.0.3 ([10]). *Let $a > 1$ and b be two positive integers. The Diophantine equation*

$$ax^2 - by^4 = 1$$

has at most one solution in positive integers (x, y).

Lemma 3.0.4. *Let D be a positive non-square integer and let $\epsilon_D = T_1 + U_1\sqrt{D}$ denote the minimal unit greater than, of norm 1 in $\mathbb{Z}[\sqrt{D}]$. For $k \geq 1$, $\epsilon_D^k = T_k + U_k\sqrt{D}$.*

1. *There are at most two positive integer solutions (X, Y) to the Diophantine equation $X^2 - DY^4 = 1$. If two solutions such that $Y_1 < Y_2$ exist, then $Y_1^2 = U_1$ and $Y_2^2 = U_2$, except only if $D = 1785$ or if $D = 16(1785)$ in which case $Y_1^2 = U_1$ and $Y_2^2 = U_4$.*

2. *If only one positive integer solution (X, Y) to the Diophantine equation $X^2 - DY^4 = 1$ exists, then $Y^2 = U_1$ where $U_1 = lv^2$ for some square-free integer l, and either $l = 1$ or $l = 2$ or $l = p$ for some prime $p \equiv 3 \pmod 4$.*

The main result proven in [16].

Theorem 3.0.5. *For any prime p and any odd positive integer $A > 1$. Then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most seven positive integer solutions (x, y).*

Proof. Let p be an odd prime, A an odd positive integer. Moreover, let x and y be positive integers verifying $y^2 = px(Ax^2 + 2)$. We consider two cases based on the parity of x.
Case 1. x is even: Then $gcd(x,\ Ax^2 + 2) = 2$. Let $x = 2z$. Since p is square free, we let $y = 2pw$ and substitute to get

$$pw^2 = z(2Az^2 + 1).$$

So there exist positive integers u, v such that $z = pu^2$ and $2Az^2 + 1 = v^2$. This gives us

$$v^2 - 2Ap^2u^4 = 1,$$

or $z = u^2$ and $2Az^2 + 1 = pv^2$ so we must have

$$pv^2 - 2Au^4 = 1.$$

Since $A > 1$ and $p > 1$ then we can use 3.0.3 to see that $pv^2 - 2Au^4 = 1$ has at most one positive integer solution (u, v). By 3.0.4, $v^2 - 2Ap^2u^4 = 1$ has at most two positive integer solutions.
Case 2. x is odd: Since p is square free, let $w = y/p$, and substitute into $y^2 = px(Ax^2 + 2)$. Giving

$$pw^2 = x(Ax^2 + 2).$$

There must exist odd integers u and v such that $x = pu^2$ and $Ax^2 + 2 = v^2$. Giving us

$$v^2 - Ap^2u^4 = 2,$$

or we get $x = u^2$ and $ax^2 + 2 = pv^2$ so we get

$$pv^2 - au^4 = 2.$$

Using 3.0.1 and 3.0.2, $pv^2 - au^4 = 2$ has at most two positive integer solutions (u, v) and by the same lemmas $v^2 - Ap^2u^4 = 2$ has at most two positive integer solutions.

□

Lemma 3.0.6 ([5], [20])**.** *Let d denote a positive non-square integer. Then the Diophantine equation*

$$dy^4 - x^2 = 1$$

has at most one positive integer solution (x, y), except when $d = 2$.

Lemma 3.0.7 ([1])**.** *Let a and b be positive integers. Then the Diophantine equation*

$$ax^4 - by^2 = 1$$

has at most two positive solutions (x, y).

Lemma 3.0.8. *For any positive odd integers a, b the Diophantine equation $aX^4 - bY^2 = 2$ has at most one solution in positive integers. Such solution must arise from the fundamental solution to quadratic equation $aX^2 - bY^2 = 2$*

The main result proven in [18]

Theorem 3.0.9. *For any prime p and any odd positive integer $A > 1$ one of the following holds:*

- *If $(A, p) \equiv (3, 1), (1, 7), (5, 3) (mod\ 8)$ then the Diophantine equation $y^2 = px(Ax^2 - 2)$ has at most two positive integer solutions (x, y).*
- *If $(A, p) \equiv (3, 5), (1, 1), (7, 5), (5, 1) (mod\ 8)$ then the Diophantine equation $y^2 = px(Ax^2 - 2)$ has at most three positive integer solutions (x, y).*
- *If $(A, p) \equiv (3, 3), (3, 7), (1, 5), (1, 3) (mod\ 8)$ then the Diophantine equation $y^2 = px(Ax^2 - 2)$ has at most one positive integer solution (x, y).*
- *Otherwise the Diophantine equation $y^2 = px(Ax^2 - 2)$ has no positive integer solutions.*

Proof. Let p be a prime, A an odd positive integer. Moreover, let x, y be positive integers satisfying $y^2 = px(Ax^2 - 2)$. If $p = 2$, then we have $x = 2x_1$ and $y = 2y_1$. Yielding $y_1^2 = 2x_1(2Ax_1^2 - 1)$.

Since $gcd(x_1, 2Ax_1^2 - 1) = 1$ we get $x_1 = 2a^2$ and $2Ax_1^2 - 1 = b^2$. Modulo 8, this cannot happen.

Assume p is and odd prime, we consider two cases based on the parity of x. Case 1. x is even: Let $x = 2z$. Since p is square free, let $w = y/2p$ and substitute to get

$$pw^2 = z(2Az^2 - 1).$$

Then there exist two positive integers u, v such that $z = pu^2$ and $2Az^2 - 1 = v^2$. This give us

$$2Ap^2u^4 - v^2 = 1,$$

or $z = u^2$ and $2Az^2 - 1 = pv^2$ giving us

$$2Au^4 - pv^2 = 1.$$

Either way, by 3.0.6, $2Ap^2u^4 - v^2 = 1$ has at most one positive integer solution (u, v). $2Ap^2u^4 - v^2 = 1$ has a positive integer solution (u, v) only if $A \equiv 1 \ (mod\ 8)$. By 3.0.7 we can see that $2Au^4 - pv^2 = 1$ has at most two positive integer solutions (u, v) and has a positive integer solution (u, v) only when $2A \equiv p + 1 \ (mod\ 8)$.
Case 2. x is odd: Since p is square-free, let $w = y/p$ and substitute to get

$$pw^2 = x(Ax^2 - 2).$$

There exists odd integers u, v such that $x = pu^2$ and $Ax^2 - 2 = v^2$ this gives us

$$Ap^2u^4 - v^2 = 2,$$

or $x = u^2$ and $Ax^2 - 2 = pv^2$ giving us

$$Au^4 - pv^2 = 2.$$

Either way, we use 3.0.8 to see $Ap^2u^4 - v^2 = 2$ or $Au^4 - pv^2 = 2$ has at most one positive integer solution (u, v). Moreover $Ap^2u^4 - v^2 = 2$ has a positive integer solution (u, v) only when $A \equiv 3 \ (mod\ 8)$. $Au^4 - pv^2 = 2$ has a positive integer solution (u, v) only if $A \equiv p + 2 \ (mod\ 8)$.

From here we can now start counting when we have zero, one, two, or three solutions. We break this up based on A. First let's give some easy names to the 4 main equations. Call $2Ap^2u^4 - v^2 = 1$, Equation 1, and call $2Au^4 - pv^2 = 1$, Equation 2. Call $Ap^2u^4 - v^2 = 2$, Equation 3, and finally call $Au^4 - pv^2 = 2$, Equation 4.

Starting with when $A \equiv 1 \ (mod\ 8)$ equation 1 has at most one solution, equation 2 has a solution only if $p \equiv 1 \ (mod\ 8)$, equation 3 has no solutions and equation 4 has a solution only if $p \equiv 7 \ (mod\ 8)$. This means $y^2 = px(Ax^2 - 2)$ has at most two positive solutions when $p \equiv 7 \ (mod\ 8)$ and has three solutions when $p \equiv 1 \ (mod\ 8)$.

When $A \equiv 3 \ (mod\ 8)$ then equation 1 has no solutions, equation 2 has a solution only when $p \equiv 5 \ (mod\ 8)$, equation 3 has at most one solution and equation 4 has a solution only when $p \equiv 1 \ (mod\ 8)$. So $y^2 = px(Ax^2 - 2)$ has at most two solution when $p \equiv 1 \ (mod\ 8)$ and it has three solutions when $p \equiv 5 \ (mod\ 8)$.

When $A \equiv 5 \ (mod\ 8)$ equation 1 and equation 3 have no solutions. Equation 2 has a solution only if $p \equiv 1 \ (mod\ 8)$ and equation 4 has a solution only if $p \equiv 3 \ (mod\ 8)$. So $y^2 = px(Ax^2 - 2)$ has has at most one solution when $p \equiv 3 \ (mod\ 8)$ and at most two solutions when $p \equiv 1 \ (mod\ 8)$.

Finally when $A \equiv 7 \ (mod\ 8)$ equation 1 and equation 3 have no solutions. Equation 2 and equation 4 only have a solution when $p \equiv 5 \ (mod\ 8)$. So $y^2 = px(Ax^2 - 2)$ has at most three solutions when $p \equiv 5 \ (mod\ 8)$. □

Lemma 3.0.10. *Let $d > 2$ be a square-free integer such that the Diophantine equation $x^2 - dy^2 = -1$ is solvable in positive integers and let $\tau = v + u\sqrt{d}$ denote its fundamental solution. The only possible integer solution to the equation $x^2 - dy^2 = -1$ is $(x, y) = (v, \sqrt{u})$.*

The main results proven in [19]

Theorem 3.0.11. *For any prime p and any square free positive integer $A > 1$, then the Diophantine equation $y^2 = px(Ax^2 \pm 1)$ has at most three positive integer solutions (x, y). Moreover, if $p = 1$ then the Diophantine equation $y^2 = px(Ax^2 \pm 1)$ has at most two positive integer solutions (x, y)*

Proof. We are going to break the proof up into three parts. One for $y^2 = px(Ax^2 + 1)$, one for $y^2 = px(Ax^2 - 1)$, and one for $y^2 = x(Ax^2 \pm 1)$

1. For $y^2 = px(Ax^2 + 1)$, let p be an odd prime, let A be a positive integer. Let x, y be positive integers verifying $y^2 = px(Ax^2 + 1)$. Consider two cases based on the parity of x.

   Case 1. x is even: Then y is also even. So replace $x = 2x_1$ and $y = 2y_1$ yielding
   $$2y_1^2 = px_1(4Ax_1^2 + 1).$$
   Since p is prime, then x_1 is even. Replacing $x_1 = 2x_2$ we get
   $$y_1^2 = px_2 = (16Ax_2^2 + 1).$$
   Replace $y = pw$ to get
   $$pw^2 = x_2(16A_2^2 + 1),$$
   Breaking this apart we know there must be positive integers u and v such that $x_2 = pu^2$ and $16Ax_2^2 + 1 = v^2$ giving us
   $$v^2 - Ap^2(au)^4 = 1.$$
   or we could have $x_2 = u^2$ and $16Ax_2^2 + 1 = pv^2$ so
   $$pv^2 - A(2u)^4 = 1.$$

   Case 2. x is odd: p is a prime number, taking $y = pW$, then substituting into $y^2 = px(Ax^2 + 1)$ we get
   $$pW^2 = x(Ax^2 + 1).$$
   This means there are integers U, V such that $x = pU^2$ and $Ax^2 + 1 = V^2$ giving us
   $$V^2 - Ap^2U^4 = 1,$$

or $x = U^2$ and $Ax^2 + 1 = pV^2$ giving us

$$pV^2 - AU^4 = 1.$$

Both equations $v^2 - Ap^2(2u)^4 = 1$ and $V^2 - Ap^2U^4 = 1$ have the right type to use 3.0.4 there are at most two solutions satisfying these equations. By 3.0.3 $pv^2 - A(2u)^4 = 1$ and $pV^2 - AU^4 = 1$ have at most one solution.

2. For $y^2 = px(Ax^2 - 1)$ similar to above, break it into cases based on parity of x.

   Case 1. x is even: Then we do the exact same thing as above, except we substitute it into $y^2 = px(Ax^2 - 1)$. This will yield

   $$Ap^2(2u)^4 - v^2 = 1.$$

   For u, v as positive integers. Flipping the values, the other equation you will get is

   $$A(su)^4 - pv^2 = 1.$$

   for u, v as positive integers.

   Case 2. x is odd: Again we do the exact same thing, just substitute it into $y^2 = px(Ax^2 - 1)$. Yielding

   $$Ap^2U^4 - V^2 = 1,$$

   and

   $$AU^4 - pV^2 = 1,$$

   for U, V as positive integers and U is odd.

   Then we use 3.0.7 on $Ap^2(2u)^4 - v^2 = 1$ and on $Ap^2U^4 - V^2 = 1$ to see each has at most one positive integer solution. And the same lemma to see $A(su)^4 - pv^2 = 1$ and $AU^4 - pV^2 = 1$ have at most two positive integer solutions.

3. For $y^2 = x(Ax^2 \pm 1)$ we do similar to above to reduce this to the two equations

   $$v^2 - Au^4 = -1,$$

   and

   $$V^2 - AU^4 = 1.$$

   Using 3.0.4, equation $V^2 - AU^4 = 1$ has at most two positive integer solutions. And use 3.0.10 to see $v^2 - Au^4 = -1$ has at most one solution.

□

Theorem 3.0.12. *For any integer $n > 1$ and any non-square positive integer $A > 1$, the Diophantine equation $y^2 = nx(Ax^2 + 1)$ has at most $2^{\omega(n)} + 1$ positive integer solutions (x, y) and the Diophantine equation $y^2 = nx(Ax^2 - 1)$ has at most $2^{\omega(n)} - 1$ positive integer solutions (x, y) where $\omega(n)$ is the number of distinct prime divisors of n*

Proof. If $n = n'm^2$, $1 < m$, $n' \in \mathbb{N}$ we can rewrite the Diophantine equation $y^2 = nx(Ax^2 \pm 1)$ to

$$y'^2 = n'x(Ax^2 \pm 1)$$

by mapping $y/m \to y'$. Assuming n is square free. This leads us to $y = nW$ and

$$x(Ax^2 \pm 1) = nW^2$$

For each divisor n_1 of n, let $n_2 = n/n_1$. Factoring we get

$$x = n_1U^2$$

and

$$Ax^2 \pm 1 = n_2V^2$$

Giving

$$An_1^2U^4 - n_2V^2 = \mp 1$$

where U, V are positive integers.

If $n_2 = 1$, by 3.0.4 and 3.0.10 there are at most two and one positive integer solutions to the equations with negative, and positive case, respectively. A square-free integer n has $2^{\omega(n)}$ divisors d and there are exactly $2^{\omega(n)} - 1$ divisors $d > 1$.

Therefore using 3.0.3 we can see $An_1^2U^4 - n_2V^2 = -1$ has at most one positive integer solution and there are most two positive integer solutions to $an_1^2U^4 - n_2V^2 = 1$, by 3.0.7.

Therefore there are at most $2^{\omega(n)-1+2}$ and $2(2^{\omega(n)} - 1) + 1$ positive integer solutions to the Diophantine equations $y^2 = nx(Ax^2 + 1)$ and $y^2 = nx(Ax^2 - 1)$ respectively. For any given $n_1 \neq n$ one of the two equations $An_1^2X^2 - n_2Y^2 = 1$ and $An_1^2X^2 - n_2Y^2 = -1$ has no integer solutions. □

Lemma 3.0.13. *If a and b are odd positive integers, then the Diophantine equation $ax^2 - by^4 = 2$ has at most two solutions in positive integers (x, y).*

Theorem 3.0.14. *For any square free positive integer n and any odd positive integer $A > 1$, the Diophantine equation $y^2 = nx(Ax^2+2)$ has at most $3(2^{\omega(x)})+1$ positive integer solutions (x, y).*

Proof. Let n be a positive square-free integer, A be an odd positive integer. Let x, y be positive integers verifying the Diophantine equation $y^2 = nx(Ax^2 + 2)$. Consider the two cases based on the parity of x.
Case 1. x is even: Then $gcd(x, ax^2 + 2) = 2$. Put $x = 2z$. Since n is square-free, we put $n = n_1n_2$, where $gcd(n_1.n_2) = 1$, then $y = 2n_1n_2w$ and we have

$$n_1n_2w^2 = z(2Az^2 + 1).$$

Then there are positive integers u, v such that $z = n_1u^2$ and $2Az^2 + 1 = n_2v^2$, which gives us

$$n_2v^2 - 2An_1^2u^4 = 1.$$

Since $A > 1$, then if $n_2 > 1$, using 3.0.3 we see $n_2v^2 - 2An_1^2u^4 = 1$ has at most one positive integer solution (u, v). If $n_2 = 1$, by 3.0.4 the equation $n_2v^2 - 2An_1^2u^4 = 1$ has at most two positive integer solutions. Since the number of factors d of a square-free n is $2^{\omega(n)}$, so the equation $y^2 = nx(Ax^2 + 2)$ has at most $(2^{\omega(x)} - 1) + 2 = 2^{\omega(x)} + 1$ positive integer solutions.
Case 2. x is odd: Since x is square-free, taking $w = \frac{y}{n_1n_2}$ we see that $y^2 = nx(Ax^2 + 2)$ gives

$$n_1n_2w^2 = x(Ax^2 + 2).$$

Then there exist odd integers u, v such that $x = n_1u^2$ and $Ax^2 + 2 = n_2v^2$ giving

$$n_2v^2 - An_1^2u^4 = 2.$$

By 3.0.13 $n_2v^2 - An_1^2u^4 = 2$ has at most two positive integer solutions (u, v). So the Diophantine equation $y^2 = nx(Ax^2 + 2)$ has at most $2(2^{\omega(x)}) = 2^{\omega(x)+1}$ positive integer solutions (u, v). □

Lemma 3.0.15 ([22])**.** *For any positive odd integers a, b, the Diophantine equation*

$$ax^4 - by^2 = 2$$

has at most one positive solution (x, y).

Theorem 3.0.16. *For any square free positive integer n and any odd positive integer $A > 1$, the Diophantine equation $y^2 = nx(Ax^2-2)$ has at most $3(2^{\omega(n)})-1$ positive integer solutions (x, y).*

Proof. The proof to this is very similar to 3.0.14. The difference being in the even case you get

$$n_2v^2 - 2An_1^2u^4 = -1.$$

And in the odd case you will get

$$n_2v^2 - An_1^2u^4 = -2.$$

Then use 3.0.10, 3.0.7, and 3.0.15 to see $n_2v^2 - 2An_1^2u^4 = -1$ has at most one positive integer solution if $n_1 = 1$ and two positive integer solutions if $n_2 > 1$. $n_2v^2 - An_1^2u^4 = -2$ has at most two positive integer solutions. So the Diophantine equation $y^2 = nx(Ax^2 - 2)$ has at most $3(2^{\omega(x)}) - 1$ positive integer solutions (x, y) □

Chapter 4

Results from The Number of Solutions to the Diophatine equation $y^2 = px(Ax^2 + 2)$

This paper was used heavily in the writing of the new results. The proofs of the new results are very similar to that of these to follow. Some notation in this section, Let a and b be odd positive integers for which the equation $aX^2 - bY^2 = 2$ has a solution in the positive integers (X, Y). Let (a_1, b_1) be the minimal positive solution to this equation and let $\alpha = \frac{a_1\sqrt{a}+b_1\sqrt{b}}{\sqrt{2}}$. For an odd integer k, define a_k and b_k to be $\alpha^k = \frac{a_k\sqrt{a}+b_k\sqrt{b}}{\sqrt{2}}$. Luca and Walsh proved the following result in [12] regarding solutions to the equation

Lemma 4.0.1. *Let D be a positive non-square integer. Suppose that $D = 2d$ where d is a positive integer different from 8(1785). Then the Diophantine equation $X^2 - DY^4 = 1$ has at most one positive solution.*

Garici, Kihel, and Larone proved the following:

Theorem 4.0.2. *Let p be a prime and let $A > 1$ be an odd integer.*

1. *If $p = 2$, then the Diophantine equation $y^2 = px(Ax^2+2)$ has at most one positive integer solution (x, y).*
2. *Suppose that $p|A$ or $(\frac{-2A}{p}) = -1$ where p is odd.*
   - *If $(A, p) \equiv (7, 1)$ or $(7, 7)$ $(mod\ 8)$, then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most three positive solutions (x, y).*
   - *Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most one positive integer solution (x, y) otherwise.*

3. *Suppose that* $(\frac{-2A}{p}) = 1$ *where* p *is odd*

- *If* $(A, p) \equiv (1,5), (1,7), (3,3), (5,5), (7,3), or\ (7,5)\ (mod\ 8)$ *then the Diophantine equation* $y^2 = px(Ax^2 + 2)$ *has at most one positive integer solution* (x, y).
- *If* $(A, p) \equiv (1,1), (3,1), (3,7), (5,1), (5,3), or\ (5,7)\ (mod\ 8)$ *then the Diophantine equation* $y^2 = px(Ax^2 + 2)$ *has at most two positive integer solutions* (x, y).
- *If* $(A, p) \equiv (1,3), or\ (3,5)\ (mod\ 8)$ *then the Diophantine equation* $y^2 = px(Ax^2 + 2)$ *has at most three positive integer solutions* (x, y).
- *If* $(A, p) \equiv (7,7)\ (mod\ 8)$ *then the Diophantine equation* $y^2 = px(Ax^2 + 2)$ *has at most four positive integer solutions* (x, y).
- *If* $(A, p) \equiv (7,1)\ (mod\ 8)$ *then the Diophantine equation* $y^2 = px(Ax^2 + 2)$ *has at most six positive integer solutions* (x, y).

Proof. Let $p = 2$ and let A be a odd positive integer. Let x, y be positive integers such that $y^2 = 2x(Ax^2+2)$. 4 divides x and y so let $y = 4w$ and $x = 4z$ to yield

$$w^2 = z(8Az^2 + 1).$$

Since $\gcd(z, 8Az^2 + 1) = 1$ there exist two positive integers u and v such that $z = u^2$ and $v^2 = 8Az^2 + 1$ giving

$$v^2 - 8Au^4 = 1.$$

F0rom 4.0.1 we know this has at most one positive integer solution (u, v).

Let p be an odd prime and let A be an odd positive integer. Let x, y be positive integers such that $y^2 = px(Ax^2 + 2)$. The $gcd(x, Ax^2 + 2) = 1$ or 2 so we have two cases based on the parity of x.
Case 1. x is even: Let $x = 2z$ and $y = 2pw$ since p is odd. Then

$$pw^2 = z(2Az^2 + 1).$$

The $gcd(z, 2Az^2 + 1) = 1$ so there exist positive integers u and v such that $z = pu^2$, $2Az^2 + 1 = v^2$ and

$$v^2 - 2Ap^2u^4 = 1.$$

Which we can let $D = 2Ap^2$ and use 4.0.1 to see this has at most one positive integer solution. There is also $z = u^2$ and $2Az^2 + 1 = pv^2$ which gives

$$pv^2 - 2Au^4 = 1.$$

Which means this has at most one positive integer solution by 3.0.3. In this case v is odd and u is even if and only if $p \equiv 1\ (mod\ 8)$. If $p \equiv 3,\ 5,$ or $7\ (mod\ 8)$ then u is odd and $p - 2A \equiv 1\ (mod\ 8)$. $pv^2 - 2Au^4 = 1$ has a solution if and only if $(\frac{-2A}{p}) = 1$ and $(A, p) \equiv (1,1), (3,1), (5,1), (7,1), (1,3), (5,3), (3,7),$ or $(7,7)\ (mod\ 8)$ that completes if x is even.

Case 2. x is odd: Then we use a similar gcd argument on

$$pw^2 = x(Ax^2 + 2),$$

to get the following two equations with odd u and v

$$v^2 - Ap^2u^4 = 2$$

and

$$pv^2 - Au^4 = 2.$$

We use 4.0.1 on both of them and reduce the first one we find $(\frac{2}{p}) = 1$ which gives us $p \equiv 1 or 7 \ (mod\ 8)$ and $v^2 - Ap^2u^4 = 2$ have a solution if and only if $(A, p) \equiv (7, 1)$, or $(7, 7)$ $(mod\ 8)$.

$pv^2 - Au^4 = 2$ is a little different. Using 3.0.2 we know this has two positive integer solutions. Since u and v are both odd we have

$$p - A \equiv 2 \ (mod\ 8).$$

So $pv^2 - Au^4 = 2$ has a solution only if $(A, p) \equiv (1, 3), (3, 5), (5, 7)$, or $(7, 1)$ $(mod\ 8)$.

Assume $pv^2 - Au^4 = 2$ has two solutions. Let (a_1, b_1) be the minimal solution to $pX^2 - AY^2 = 2$ so

$$pa_1^2 - Ab_1^2 = 2.$$

Using $\alpha = \frac{a_1\sqrt{a} + b_1\sqrt{b}}{\sqrt{2}}$, calculate the cube to get

$$b_3 = \frac{3\alpha_1^2 pb_1 + b_1^3 A}{2}.$$

3.0.2 and our assumption of two solutions existing tells us that b_1 and b_3 are both squares. So there exists two positive integers B_1 and B_3 such that $b_1 = B_1^2$ and $b_3 = B_3^2$ and we can substitute that into $b_3 = \frac{3\alpha_1^2 pb_1 + b_1^3 A}{2}$ to get

$$2B_3^2 = 3a_1^2 pB_1^2 + B_1^6 A.$$

This yields $(\frac{2}{p}) = (\frac{A}{p})$. Since $-Au^4 \equiv 2 \ (mod\ p)$ we get $(\frac{-A}{p}) = (\frac{2}{p}) = (\frac{A}{p})$ so $(\frac{-1}{p}) = 1$. That means $p \equiv 1 \ (mod\ 4)$ so $p \equiv 1$ or $5 \ (mod\ 8)$.

$pv^2 - Au^4 = 2$ has at most two positive integer solutions only if $(A, p) \equiv (3, 5)$ or $(7, 1)$ $(mod\ 8)$ and it only has one solution if $(A, p) \equiv (1, 3)$ or $(5, 7)$ $(mod\ 8)$ and it has a solution only if $(\frac{-2A}{p}) = 1$.

Since $pv^2 - 2Au^4 = 1$ and $pv^2 - Au^4 = 2$ depend on the value of $(\frac{-2A}{p})$. If $p|A$ or $(\frac{-2A}{p}) = -1$. $pv^2 - 2Au^4 = 1$ and $pv^2 - Au^4 = 2$ have no integer solutions. $pw^2 = z(2Az^2 + 1)$ has at most one solution and $v^2 - Ap^2u^4 = 2$ has at most two solutions but only if $(A, p) \equiv (7, 1)$, or $(7, 7)$ $(mod\ 8)$. This means that when $p|A$ or $\frac{-2A}{p} = -1$ then $y^2 = px(Ax^2 + 2)$ has at most three positive solutions if $(A, p) \equiv (7, 1)$, or $(7, 7)$ $(mod\ 8)$ and has at most one solution otherwise.

When $(\frac{-2A}{p}) = 1$ then we know $pv^2 - 2Au^4 = 1$ has at most one positive integer solution but only if p is certain values $(mod\ 8)$. Also in the following cases we know that $v^2 - 2Ap^2u^4 = 1$ has one solution. The rest we split up on the value of A reduced by $(mod\ 8)$.

If $A \equiv 1\ (mod\ 8)$ then only if $p \equiv 1$ or $3\ (mod\ 8)$ does $pv^2 - 2Au^4 = 1$ have at most one solution. $v^2 - Ap^2u^4 = 2$ has no solutions and $pv^2 - Au^4 = 2$ has at most one solution but only if $p \equiv 3\ (mod\ 8)$.

If $A \equiv 3\ (mod\ 8)$ then only if $p \equiv 1$ or $7\ (mod\ 8)$ does $pv^2 - 2Au^4 = 1$ have at most one solution. $v^2 - Ap^2u^4 = 2$ has no solutions and $pv^2 - Au^4 = 2$ has at most two solutions but only if $p \equiv 5\ (mod\ 8)$.

If $A \equiv 5\ (mod\ 8)$ then only if $p \equiv 1$ or $5\ (mod\ 8)$ does $pv^2 - 2Au^4 = 1$ have at most one solution. $v^2 - Ap^2u^4 = 2$ has no solutions and $pv^2 - Au^4 = 2$ has at most one solution but only if $p \equiv 7\ (mod\ 8)$.

If $A \equiv 7\ (mod\ 8)$ then only if $p \equiv 1$ or $7\ (mod\ 8)$ does $pv^2 - 2Au^4 = 1$ have at most one solution. $v^2 - Ap^2u^4 = 2$ has at most two solutions but only if $p \equiv 1$ or $7\ (mod\ 8)$ and $pv^2 - Au^4 = 2$ has at most one solution but only if $p \equiv 1\ (mod\ 8)$.

□

Theorem 4.0.3. *Let p be a prime and let $A > 1$ be an even integer.*

1. *If $p = 2$, then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most two positive integer solutions (x, y). Moreover, if $A \equiv 0\ (mod\ 4)$ and $A \neq 2^6(1785)$, then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most one positive integer solution (x, y).*

2. *Suppose that $p|A$ or $(\frac{-2A}{p}) = -1$ where p is odd.*

   - *If $A \equiv 0\ (mod\ 4)$, then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most one positive solution (x, y).*
   - *If $A \equiv 2\ (mod\ 4)$, then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most two positive solutions (x, y).*

3. *Suppose that $(\frac{-2A}{p}) = 1$ where p is odd.*

   - *If $(A, p) \equiv (0, 3)\ (mod\ 4)$ then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most one positive integer solution (x, y).*
   - *If $(A, p) \equiv (0, 1)\ (mod\ 4)$ then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most two positive integer solutions (x, y).*
   - *If $(A, p) \equiv (2, 3)\ (mod\ 4)$ then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most three positive integer solutions (x, y).*
   - *If $(A, p) \equiv (2, 1)\ (mod\ 8)$ then the Diophantine equation $y^2 = px(Ax^2 + 2)$ has at most four positive integer solutions (x, y).*

Proof. If A is even and p is odd, we let $A = 2A'$. Then

$$y^2 = 2px(A'x^+1).$$

Let $y = 2pw$, and we obtain

$$2pw^2 = x(A'x^2 + 1).$$

Since $gcd(x, A'x^2 + 1) = 1$, there exist positive integers u and v such that either $x = 2pu^2$, and $A'x^2 + 1 = v^2$ giving

$$v^2 - 4A'p^2u^4 = 1.$$

Or $x = 2u^2$, and $A'x^2 + 1 = pv$ giving

$$pv^2 - 4A'u^4 = 1.$$

Or $x = u^2$, and $A'x^2 + 1 = 2pv^2$ giving

$$2pv^2 - A'u^4 = 1.$$

Or $x = pu^2$, and $A'x^2 + 1 = 2v^2$ giving

$$2v^2 - A'p^2u^4 = 1.$$

If A' is a perfect square, then $v^2 - 4A'p^2u^4 = 1$ has no positive integer solution, otherwise it has at most one positive integer solution by 4.0.1.

By 3.0.3 each of $pv^2 - 4A'u^4 = 1$, $2pv^2 - A'u^4 = 1$, and $2v^2 - A'p^2u^4 = 1$ have at most one solution.

$pv^2 - 4A'u^4 = 1$ has a solution only if $p \equiv 1 \ (mod\ 4)$ and $(\frac{-A'}{p}) = 1$. $2pv^2 - A'u^4 = 1$ has a solution only if A' is odd and $(\frac{-A'}{p}) = 1$. $2v^2 - A'p^2u^4 = 1$ has a solution only if A' is odd. Since the number of solutions to $pv^2 - 4A'u^4 = 1$ and $2pv^2 - A'u^4 = 1$ depends on the value of $(\frac{-A'}{p}) = (\frac{-2A'}{p})$. We first suppose that $p|A$ or $(\frac{-2A'}{p}) = -1$. Then $pv^2 - 4A'u^4 = 1$ and $2pv^2 - A'u^4 = 1$ have no integer solution.

If $A \equiv 0 \ (mod\ 4)$, then equation $v^2 - 4A'p^2u^4 = 1$ has at most one solution $pv^2 - 4A'u^4 = 1$, $pv^2 - 4A'u^4 = 1$, and $2pv^2 - A'u^4 = 14$, have no solution.

If $A \equiv 2 \ (mod\ 4)$, then equation $v^2 - 4A'p^2u^4 = 1$ has at most one solution $pv^2 - 4A'u^4 = 1$, and $pv^2 - 4A'u^4 = 1$ have no solutions and $2pv^2 - A'u^4 = 14$ has at most one solution.

Now we suppose that $(\frac{-2A}{p}) = 1$. Then equation $v^2 - 4A'p^2u^4 = 1$ and $pv^2 - 4A'u^4 = 1$ have at most one positive integer solution.

If $A \equiv 0 \ (mod\ 4)$, then equation $v^2 - 4A'p^2u^4 = 1$ has at most one solution. $pv^2 - 4A'u^4 = 1$ has at most one solution only if $p \equiv 1 \ (mod\ 4)$. $pv^2 - 4A'u^4 = 1$, and $2pv^2 - A'u^4 = 14$ have no solution.

If $A \equiv 2 \ (mod\ 4)$, then equation $v^2 - 4A'p^2u^4 = 1$ has at most one solution. $pv^2 - 4A'u^4 = 1$ has at most one solution only if $p \equiv 1 \ (mod\ 4)$.

$pv^2 - 4A'u^4 = 1$ has at most one solution and $2pv^2 - A'u^4 = 14$ has at most one solution.

If A is even and $p = 2$, we let $A = 2A'$. Then $y^2 = 2x(2A'x^2 + 1)$. We let $y = 2w$ and we obtain $w^2 = x(A'x^2 + 1)$.

Since $gcd(x, A'x^2 + 1) = 1$, there exist positive integers u and v such that $x = u^2$ and $A'x^2 + 1 = v^2$ and $v^2 - A'u^4 = 1$ has no solution if A' is a perfect square at at most two solutions by 3.0.4. Moreover, if A' is even and $A' \neq 2^5(1785)$, then by 4.0.1 $v^2 - A'u^4 = 1$ has at most one solution.

□

Chapter 5

New Results on the Diophantine Equation $y^2 = px(Ax^2 - C),\ C \in \{2, \pm 1, \pm 4\}$

In this section, we present new bounds to the Diophantine Equation $y^2 = px(Ax^2 - C)$. This work has been submitted for publishing. Several authors of the last two hundred years have studied the integer solutions of the equation

$$x^3 + y^3 + z^3 = u^2. \tag{5.1}$$

Among them we can cite, in particular, Bouniakowsky [3] who gave in 1853 the identity

$$(3\lambda)^3 + (2 - \lambda^3)^3 + (\lambda^3 + 1)^3 = \left(3(\lambda^3 + 1)\right)^2,$$

which provides infinitely many solutions for equation (5.1). By proving a new identity similar to Bouniakowsky's one, Catalan established in 1866, another family of solutions for equation (5.1). In 1916, Gérardin [9] drew up a table of solutions for equation (5.1), unfortunately this table is not exhaustive. For more historical details, see, Dickson's classical book [7].

In 1985, Cassels [4] was challenged to find when does a sum of three consecutive cubes equal a square. He reduced the question to solving the Diophantine equation $y^2 = 3x(x^2 + 2)$, and obtained that the positive solutions are $(x, y) = (1, 3)$, $(2, 6)$, and $(24, 204)$. Luca and Walsh [13] generalized Cassels' equation and proved that the Diophantine equation $y^2 = nx(x^2 + 2)$ has at most $3(2^{\omega(n)-1})$ positive solutions, where n is a positive integer and $\omega(n)$ is the number of distinct prime divisors of n. Chen [6] improved the last result when $n = p$ is an odd prime, by proving that the Diophantine equation $y^2 = px\left(x^2 + 2\right)$ has at most two positive solutions. Togbé [16] considered the more general equation $y^2 = px\left(Ax^2 + 2\right)$, where A is an odd integer and proved that it has at most seven positive solutions.

Li and Yuan [21] considered another variant of Cassels' equation. They proved that the Diophantine equation $y^2 = px(Ax^2 - 2)$, where p is an odd prime and A is an odd integer greater than 1, has at most five positive solutions (x, y). Wu *et al.* [19] studied the equation $y^2 = px(Ax^2 - C)$, $C \in \{\pm 1, \pm 4\}$. They showed, among other results, that if p is an odd prime, then the previous equation has at most three positive solutions when $C = \pm 1$, seven positive solutions when $C = 4$, and eight positive solutions when $C = -4$.

In this section, by using reduction modulo 8, reduction modulo p and some properties of the Legendre symbol, we give new upper bounds for the number of integer positive solutions (x, y) of the Diophantine equation $y^2 = px(Ax^2 - C)$, $C \in \{2, \pm 1, \pm 4\}$, where p is an odd prime and A is an even positive integer in the cases where $C = \pm 1$ and an odd positive integer otherwise.

5.1 Preliminary Lemmas

The study of the Diophantine equation $ax^4 - by^2 = C$ was initiated by Ljunggren [10]. Later, several other authors, especially, Chen and Voutier [5], Yuan [20], Akhtari [1], and Yuan and Li [22], extended and improved the work of Ljunggren [10, 11]. In this section, we recall some well-known results on the Diophantine equation $ax^4 - by^2 = C$, where $C \in \{2, \pm 1, \pm 4\}$.

In what follows we mean by a positive solution (x, y) that both x and y are positive integers and by $(A, p) \equiv (a, b) \pmod 8$ that $A \equiv a \pmod 8$ and $p \equiv b \pmod 8$.

Lemma 5.1.1 ([8])**.** *Let D be a positive non-square integer. Suppose that $D = 2d$ where d is a positive integer different from $8(1785)$. Then the equation $x^2 - Dy^4 = 1$ has at most one positive solution (x, y).*

For the remainder of this section, we assume that the odd positive integers A and B have the property that the Diophantine equation

$$Ax^2 - By^2 = 4 \tag{5.2}$$

has solutions in odd, positive integers (x, y). Let (a_1, b_1) be the least solution of equation (5.2) in odd, positive integers. Define for integer n

$$\frac{a_n\sqrt{A} + b_n\sqrt{B}}{2} = \left(\frac{a_1\sqrt{A} + b_1\sqrt{B}}{2}\right)^n,$$

where n is a positive integer in the case $A = 1$ and an odd positive integer otherwise. Then (a_n, b_n) are all the solutions of equation (5.2) in positive integers. With these assumptions, Ljunggren [11] proved the following result

Lemma 5.1.2. *The Diophantine equation*

$$Ax^4 - By^2 = 4 \tag{5.3}$$

has at most two solutions in positive integers (x, y).

1. *If* $a_1 = h^2$ *and* $Aa_1^2 - 3 = k^2$, *there are only two solutions, namely,* $x = \sqrt{a_1} = h$ *and* $x = \sqrt{a_3} = hk$.

2. *If* $a_1 = h^2$ *and* $Aa_1^2 - 3 \neq k^2$, *then* $x = \sqrt{a_1} = h$ *is the only solution.*

3. *If* $a_1 = 5h^2$ *and* $A^2a_1^4 - 5Aa_1^2 + 5 = 5k^2$, *then the only solution is* $x = \sqrt{a_5} = 5hk$.

   Otherwise there are no solutions.

In 2007, Luo and Yuan [14] proved the following result, where $\square$ denote the square of an integer.

Lemma 5.1.3. *1. If* b_1 *is not a square, then the equation*

$$Ax^2 - By^4 = 4 \tag{5.4}$$

has no positive integer solutions except for the case $b_1 = 3\square$ *and* $Bb_1^2 + 3 = 3\square$, *when* $(x, y) = (a_3, \sqrt{b_3})$ *is the only solution of* (5.4).

2. *If* b_1 *is a square, then* (5.4) *has at most one positive integer solution other than* $(x, y) = (a_1, \sqrt{b_1})$, *which is either* $(x, y) = (a_3, \sqrt{b_3})$ *or* $(x, y) = \left(a_2, \sqrt{b_2}\right)$, *the latter occurring if and only if* a_1 *and* b_1 *are both squares and* $A = 1$, $B \neq 5$.

5.2 The Diophantine equation $y^2 = px(Ax^2 - 2)$

Togbé and Yuan [18], considered the Diophantine equation

$$y^2 = px(Ax^2 - 2), \tag{5.5}$$

where p is an odd prime and $A > 1$ an odd integer. By using reduction modulo 8, they stated some results on the bound of the number of solutions for equation (5.5). It seems there is a gap in their result. In fact, $(x, y) = (8, 892)$ is a solution of equation (5.5) for $A = 7$ and $p = 223$, which contradicts the last statement of their main theorem. In this section, in addition to reduction modulo 8, we will use reduction modulo p and some properties of Legendre symbol to prove the following result.

Theorem 5.2.1. *For any odd prime* p *and any odd integer* $A > 1$, *the Diophantine equation* (5.5) *has at most three positive integer solutions* (x, y). *Moreover, we have*

1. *Suppose that* $p \mid A$ *or* $\left(\frac{2A}{p}\right) = -1$.

   (a) *If* $(A, p) \equiv (1, 1)$, $(1, 5)$, $(3, 1)$, $(3, 3)$, $(5, 1)$ *or* $(5, 5) \pmod 8$, *then the Diophantine equation* (5.5) *has at most one positive integer solution* (x, y).

(b) *Diophantine equation* (5.5) *has no positive integer solutions* (x, y) *otherwise.*

2. *Suppose that* $\left(\frac{2A}{p}\right) = 1$.

   (a) *If* $(A, p) \equiv (1, 3)$, $(7, 1)$ *or* $(7, 3) \pmod 8$, *then the Diophantine equation* (5.5) *has no positive integer solutions* (x, y).

   (b) *If* $(A, p) \equiv (1, 5)$, $(3, 3)$, $(5, 3)$ *or* $(5, 5) \pmod 8$, *then the Diophantine equation* (5.5) *has at most one positive integer solution* (x, y).

   (c) *If* $(A, p) \equiv (3, 1)$, $(3, 5)$, $(3, 7)$, $(5, 7)$ *or* $(7, 7) \pmod 8$, *then the Diophantine equation* (5.5) *has at most two positive integer solutions* (x, y).

   (d) *If* $(A, p) \equiv (1, 1)$, $(1, 7)$, $(5, 1)$ *or* $(7, 5) \pmod 8$, *then the Diophantine equation* (5.5) *has at most three positive integer solutions* (x, y).

Proof. Let p be an odd prime, A an odd positive integer, and (x, y) a positive integer solution to $y^2 = px(Ax^2 - 2)$. As explained by Togbé and Yuan [18], there are two cases to be considered.
Suppose first that x is odd. Then there exist odd integers u and v such that $x = pu^2$, $Ax^2 - 2 = v^2$ and

$$Ap^2u^4 - v^2 = 2 \tag{5.6}$$

or $x = u^2$, $Ax^2 - 2 = pv^2$ and

$$Au^4 - pv^2 = 2. \tag{5.7}$$

If equation (5.6) has a solution, then the Legendre symbol $\left(\frac{-2}{p}\right) = 1$, which is equivalent to $p \equiv 1$ or $3 \pmod 8$. By Lemma 3.0.15, equations (5.6) and (5.7) have at most one positive solution (u, v). Clearly equation (5.6) has a solution only when $A \equiv 3 \pmod 8$, and equation (5.7) has a solution only if $A \equiv p + 2 \pmod 8$ and $\left(\frac{2A}{P}\right) = 1$.
Suppose next that x is even. Let $x = 2z$, where z is a positive integer. One obtains that there exist integers u and v such that $z = pu^2$, $2Az^2 - 1 = v^2$ and

$$2Ap^2u^4 - v^2 = 1, \tag{5.8}$$

or $z = u^2$, and $2Az^2 - 1 = pv^2$

$$2Au^4 - pv^2 = 1. \tag{5.9}$$

Lemma 3.0.6 implies that equation (5.8) has at most one positive solution. If equation (5.8) has a solution, then $\left(\frac{-1}{p}\right) = 1$, which is equivalent to $p \equiv 1 \pmod 4$. Moreover, if equation (5.8) has a solution, then u and v are both odd, and consequently $2A \equiv 2 \pmod 8$, i.e., $A \equiv 1 \pmod 4$.

Lemma 3.0.7 implies that equation (5.9) has at most two positive solutions. If equation (5.9) has a solution, then v is odd and depending on the parity of u, $p+1 \equiv 2A$ or $0 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$. Then, we have the following.

If $A \equiv 1 \pmod 8$, then equation (5.6) has no solutions, equation (5.7) has a solution only if $p \equiv 7 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$, equation (5.8) has a solution only if $p \equiv 1$ or $5 \pmod 8$, and equation (5.9) has a solution only if $p \equiv 1$ or $7 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$.

If $A \equiv 3 \pmod 8$, then equation (5.6) has a solution only when $p \equiv 1$ or $3 \pmod 8$, equation (5.7) has a solution only when $p \equiv 1 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$, equation (5.8) has no solutions, and equation (5.9) has a solution only when $p \equiv 5$ or $7 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$.

If $A \equiv 5 \pmod 8$, then equation (5.6) has no solutions, equation (5.7) has a solution only when $p \equiv 3 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$, equation (5.8) has a solution only when $p \equiv 1$ or $5 \pmod 8$, and equation (5.9) has a solution only when $p \equiv 1$ or $7 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$.

If $A \equiv 7 \pmod 8$, then equation (5.6) has no solutions, equation (5.7) has a solution only when $p \equiv 5 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$, equation (5.8) has no solutions, and equation (5.9) has a solution only when $p \equiv 5$ or $7 \pmod 8$ and $\left(\frac{2A}{p}\right) = 1$. □

5.3 The Diophantine equation $y^2 = px\left(Ax^2 \pm 1\right)$

Wu *et al.* [19] considered the Diophantine equation

$$y^2 = nx\left(Ax^2 \pm C\right). \tag{5.10}$$

In the case $n = p$, a prime, A a positive integer and $C = 1$, they noted that equation (5.10) has at most three positive solutions (x, y). We will make this result more precise in the case where A is an even positive non-square integer. We prove the following theorems.

Theorem 5.3.1. *For any odd prime p and any even positive non-square integer A, if $(A, p) \not\equiv (2, 1) \pmod 8$, then the Diophantine equation*

$$y^2 = px\left(Ax^2 - 1\right) \tag{5.11}$$

has at most two positive integer solutions (x, y). Moreover, we have the following.

1. *Suppose that* $p \mid A$ *or* $\left(\frac{A}{p}\right) = -1$.

   (a) *If* $(A, p) \equiv (2, 1)$ *or* $(2, 5) \pmod 8$, *then the Diophantine equation* (5.11) *has at most one positive integer solution* (x, y).

   (b) *Diophantine equation* (5.11) *has no positive integer solutions* (x, y) *otherwise.*

2. *Suppose that* $\left(\frac{A}{p}\right) = 1$.

   (a) *If* $(A, p) \equiv (2, 5) \pmod 8$, *then the Diophantine equation* (5.11) *has at most one positive integer solution* (x, y).

   (b) *If* $(A, p) \equiv (0, 7)$, $(2, 7)$, $(4, 3)$, $(4, 7)$, $(6, 5)$ *or* $(6, 7) \pmod 8$, *then the Diophantine equation* (5.11) *has at most two positive integer solutions* (x, y).

   (c) *If* $(A, p) \equiv (2, 1) \pmod 8$, *then the Diophantine equation* (5.11) *has at most three positive integer solutions* (x, y).

   (d) *Diophantine equation* (5.11) *has no positive integer solutions* (x, y) *otherwise.*

Theorem 5.3.2. *For any odd prime* p *and any even positive non-square integer* A, *the Diophantine equation*

$$y^2 = px\left(Ax^2 + 1\right) \tag{5.12}$$

has at most two positive integer solutions (x, y). *Moreover, equation* (5.12) *has at most one positive integer solution* (x, y) *if any of the following conditions is satisfied :*

1. $p \mid A$ *or* $\left(\frac{-A}{p}\right) = -1$.

2. $(A, p) \equiv (0, 3)$, $(0, 5)$, $(0, 7)$, $(2, 5)$, $(2, 7)$, $(4, 3)$, $(4, 7)$, $(6, 3)$ *or* $(6, 5) \pmod 8$.

Proof of Theorem 5.3.1. Let p be an odd prime, and let A be an even positive non-square integer. Let x, y be positive integers such that $y^2 = px(Ax^2 - 1)$. Since p is prime, we let $y = pw$. Then we obtain $pw^2 = x(Ax^2 - 1)$. Since $\gcd(x, Ax^2 - 1) = 1$, there exist positive integers u and v such that either $x = pu^2$, $Ax^2 - 1 = v^2$, and

$$Ap^2u^4 - v^2 = 1, \tag{5.13}$$

or $x = u^2$, $Ax^2 - 1 = pv^2$, and

$$Au^4 - pv^2 = 1. \tag{5.14}$$

We consider each of the above two equations separately to determine upper bounds for the number of positive solutions to equation (5.11).

We begin with equation (5.13). Let $d = Ap^2$. By Lemma 3.0.6, equation (5.13) has at most one positive solution (u, v). Since A is even, u and v are clearly both odd. Therefore equation (5.13) has a solution only if $A \equiv 2 \pmod 8$. Furthermore, equation (5.13) has a solution only if $\left(\frac{-1}{p}\right) = 1$, i.e. $p \equiv 1$ or $5 \pmod 8$.

We next consider equation (5.14). By Lemma 3.0.7, this equation has at most two positive solutions(u, v). It follows that v is odd and depending on the parity of u, $p+1 \equiv A$ or $0 \pmod 8$. Then equation (5.14) has a solution only if $(A, p) \equiv (0, 7)$, $(2, 1)$, $(2, 7)$, $(4, 3)$, $(4, 7)$, $(6, 5)$ or $(6, 7) \pmod 8$. Furthermore, equation (5.14) has a solution only if $\left(\frac{A}{p}\right) = 1$. □

Proof of Theorem 5.3.2. Let p be an odd prime, and let A be an even positive non-square integer. Let x, y be positive integers such that $y^2 = px(Ax^2 + 1)$. Since p is prime, we let $y = pw$. Then we obtain

$$pw^2 = x(Ax^2 + 1).$$

Since $\gcd(x, Ax^2 + 1) = 1$, there exist positive integers u and v such that either $x = pu^2$, $Ax^2 + 1 = v^2$, and

$$v^2 - Ap^2u^4 = 1, \tag{5.15}$$

or $x = u^2$, $Ax^2 + 1 = pv^2$, and

$$pv^2 - Au^4 = 1. \tag{5.16}$$

We consider each of the above two equations separately to determine upper bounds for the number of positive solutions to equation (5.12).

We begin with equation (5.15). Let $D = Ap^2$. Since p is an odd prime and $p^2 \mid D$ then $D \neq 16(1785)$. By Lemma 5.1.1, equation (5.15) has at most one positive solution.

We next consider equation (5.16), which has at most one positive solution by Lemma 3.0.3. If equation (5.16) has a solution (u, v), then v is odd and depending on the parity of u, $p - 1 \equiv A$ or $0 \pmod 8$. Then equation (5.16) has a solution only if $(A, p) \equiv (0, 1)$, $(2, 1)$, $(2, 3)$, $(4, 1)$, $(4, 5)$, $(6, 1)$ or $(6, 7) \pmod 8$. Furthermore, equation (5.16) has a solution only if $\left(\frac{-A}{p}\right) = 1$. □

5.4 The Diophantine equation $y^2 = px(Ax^2 \pm 4)$

Wu *et al.* [19] considered the Diophantine equations

$$y^2 = nx(Ax^2 - 4), \tag{5.17}$$

$$y^2 = nx(Ax^2 + 4), \tag{5.18}$$

where n is a square free positive integer and A an odd positive integer. In the case $n = p$ an odd prime, they proved that the Diophantine equation (5.17) has at most eight positive solutions (x, y) and the Diophantine equation (5.18) has at most seven positive solutions (x, y). In this section, we will improve this result by proving the following two theorems.

Theorem 5.4.1. *If A is a positive odd integer and p is an odd prime, then the Diophantine equation*

$$y^2 = px(Ax^2 - 4) \tag{5.19}$$

has at most six positive integer solutions. Moreover, we have the following.

1. *Suppose that $p \mid A$ or $\left(\frac{A}{p}\right) = -1$.*
   (a) *If $(A, p) \equiv (1, 1)$, $(1, 3)$, $(3, 1)$ or $(3, 3) \pmod 8$, then the Diophantine equation (5.19) has at most two positive integer solutions (x, y).*
   (b) *If $(A, p) \equiv (5, 1)$ or $(5, 5) \pmod 8$, then the Diophantine equation (5.19) has at most one positive integer solution (x, y).*
   (c) *Diophantine equation (5.19) has no positive integer solutions (x, y) otherwise.*
2. *Suppose that $\left(\frac{A}{p}\right) = 1$.*
   (a) *If $(A, p) \equiv (1, 3) \pmod 8$, then the Diophantine equation (5.19) has at most six positive integer solutions (x, y).*
   (b) *If $(A, p) \equiv (1, 1)$, $(1, 7)$, $(3, 3)$, $(3, 1)$, $(7, 3)$ or $(7, 7) \pmod 8$, then the Diophantine equation (5.19) has at most four positive integer solutions (x, y).*
   (c) *If $(A, p) \equiv (1, 5) \pmod 8$, then the Diophantine equation (5.19) has at most three positive integer solutions (x, y).*
   (d) *If $(A, p) \equiv (3, 5)$, $(3, 7)$, $(5, 1)$, $(5, 3)$ or $(5, 7) \pmod 8$, then the Diophantine equation (5.19) has at most two positive integer solutions (x, y).*
   (e) *If $(A, p) \equiv (5, 5) \pmod 8$, then the Diophantine equation (5.19) has at most one positive integer solution (x, y).*
   (f) *If $(A, p) \equiv (7, 1)$ or $(7, 5) \pmod 8$, then the Diophantine equation (5.19) has no positive integer solution (x, y).*

Proof. Let A be a positive odd integer, p an odd prime and (x, y) a positive solution to $y^2 = px(Ax^2 - 4)$. Since p is prime, we let $y = pw$. Then we obtain

$$pw^2 = x(Ax^2 - 4).$$

Suppose first that $p \mid x$. Let $x = pz$. Then

$$w^2 = z\left(Ap^2z^2 - 4\right).$$

Two cases may arise. z and $\left(Ap^2z^2-4\right)$ are either perfect squares or not. Since $\gcd(z, Ap^2z^2-4) = 1$, 2 or 4, then there exist integers u and v such that $z = u^2$ and

$$Ap^2u^4 - v^2 = 4, \tag{5.20}$$

or $z = 2u^2$ and

$$Ap^2u^4 - 2v^2 = 1. \tag{5.21}$$

Suppose next that $(p, x) = 1$. As was explained previously, there exist integers u and v such that $x = u^2$ and

$$Au^4 - pv^2 = 4, \tag{5.22}$$

or $x = 2u^2$ and

$$Au^4 - 2pv^2 = 1. \tag{5.23}$$

Suppose that equation (5.20) has a solution (u, v). If u and v are both even, by considering equation (5.20) modulo 16. We obtain the absurdity that -4 is quadratic residue modulo 16. If equation (5.20) has a solution in odd integers u, v, then $A \equiv 5 \pmod 8$ and $\left(\frac{-1}{p}\right) = 1$, which is equivalent to $p \equiv 1$ or $5 \pmod 8$. Moreover, by Lemma 5.1.2, equation (5.20) has at most one solution in odd positive integers.

Lemma 3.0.7 implies that equation (5.21) has at most two positive solutions. If equation (5.21) has a solution, then $\left(\frac{-2}{p}\right) = 1$, which is equivalent to $p \equiv 1$ or $3 \pmod 8$. Moreover, if equation (5.21) has a solution, then u is odd, and consequently $A \equiv 1$ or $3 \pmod 8$.

Lemma 3.0.7 and Lemma 5.1.2 imply that equation (5.22) has at most two positive solutions. If $p \equiv 1$ or $5 \pmod 8$, then equation (5.22) has no solutions in even positive integers u, v, and by Lemma 5.1.2, has at most one positive solution in odd integers u, v only if $A \equiv p + 4 \pmod 8$. Moreover, equation (5.22) has a solution only if $\left(\frac{A}{p}\right) = 1$.

Lemma 3.0.7 implies that equation (5.23) has at most two positive solutions. If equation (5.23) has a solution, then u is odd and depending on the parity of v, $A \equiv 1$ or $1 + 2p \pmod 8$ and $\left(\frac{A}{p}\right) = 1$.

If $A \equiv 1 \pmod 8$, then equation (5.20) has no solutions, equation (5.21) has at most two positive solutions only if $p \equiv 1$ or $3 \pmod 8$, equation (5.22) has no solutions if $p \equiv 1 \pmod 8$, at most one positive solution if $p \equiv 5 \pmod 8$ and at most two positive solutions otherwise. Equation (5.23) has at most two positive solutions.

If $A \equiv 3 \pmod 8$, then equation (5.20) has no solutions, equation (5.21) has at most two positive solutions only if $p \equiv 1$ or $3 \pmod 8$, equation (5.22) has at

most two positive solutions only when $p \equiv 3$ or $7 \pmod 8$, and equation (5.23) has at most two positive solutions only when $p \equiv 1$ or $5 \pmod 8$.

If $A \equiv 5 \pmod 8$, then equation (5.20) has at most one positive solution only when $p \equiv 1$ or $5 \pmod 8$, equations (5.21) and (5.23) have no solutions, equation (5.22) has at most one positive solution if $p \equiv 1 \pmod 8$, at most two positive solutions when $p \equiv 3$ or $7 \pmod 8$, and no solutions when $p \equiv 5 \pmod 8$.

If $A \equiv 7 \pmod 8$, then equations (5.20) and (5.21) have no solutions and equations (5.22) and (5.23) have at most two positive solutions only when $p \equiv 3$ or $7 \pmod 8$.

Moreover, equations (5.22) and (5.23) have solutions only if $\left(\frac{A}{p}\right) = 1$.

□

Theorem 5.4.2. *If A is a positive odd integer and p is an odd prime, then the Diophantine equation*

$$y^2 = px(Ax^2 + 4) \tag{5.24}$$

has at most four positive integer solutions. Moreover, we have the following.

1. *Suppose that $p \mid A$ or $\left(\frac{-A}{p}\right) = -1$.*
   (a) *If $(A, p) \equiv (1,1), (1,7), (5,1), (5,3), (5,5), (5,7), (7,1)$ or $(7,7) \pmod 8$, then the Diophantine equation (5.24) has at most two positive integer solutions (x, y).*
   (b) *Diophantine equation (5.24) has at most one positive integer solution (x, y) otherwise.*
2. *Suppose that $\left(\frac{-A}{p}\right) = 1$.*
   (a) *If $(A, p) \equiv (1,1), (1,5), (5,1)$ or $(7,1) \pmod 8$, then the Diophantine equation (5.24) has at most four positive integer solutions (x, y).*
   (b) *If $(A, p) \equiv (5,3), (5,5), (5,7), (7,3), (7,5)$ or $(7,7) \pmod 8$, then the Diophantine equation (5.24) has at most three positive integer solutions (x, y).*
   (c) *If $(A, p) \equiv (1,7), (3,1), (3,5)$ or $(3,7) \pmod 8$, then the Diophantine equation (5.24) has at most two positive integer solutions (x, y).*
   (d) *If $(A, p) \equiv (1,3)$ or $(3,3) \pmod 8$, then the Diophantine equation (5.24) has at most one positive integer solution (x, y).*

Proof. Let A be a positive odd integer, p an odd prime and (x, y) a positive solution to $y^2 = px(Ax^2 + 4)$. As was explained in the proof of Theorem 5.4.1, there exist integers u and v such that $x = pu^2$ and

$$v^2 - Ap^2u^4 = 4, \tag{5.25}$$

or $x = 2pu^2$ and

$$2v^2 - Ap^2u^4 = 1, \tag{5.26}$$

or $x = u^2$ and

$$pv^2 - Au^4 = 4, \tag{5.27}$$

or $x = 2u^2$ and

$$2pv^2 - Au^4 = 1. \tag{5.28}$$

Lemma 5.1.3 implies that if equation $X^2 - Ap^2Y^2 = 4$ has a solution in odd positive integers, then equation (5.25) has at most two solutions in odd positive integers. Lemma 5.1.1 implies that equation (5.25) has at most one solution in even positive integers. Equation (5.25) has a solution in odd positive integers only if $A \equiv 5 \pmod 8$.

Lemma 3.0.3 implies that equation (5.26) has at most one positive solution. If equation (5.26) has a solution, then $\left(\frac{2}{p}\right) = 1$, which is equivalent to $p \equiv 1$ or $7 \pmod 8$. Moreover, if equation (5.26) has a solution, then u is odd, and depending on the parity of v, $A \equiv 1$ or $7 \pmod 8$.

Lemma 5.1.3 implies that if equation $pX^2 - AY^2 = 4$ has a solution in odd positive integers, then equation (5.27) has at most one solution in odd positive integers, and at most one solution in even positive integers. Lemma 3.0.3 implies that equation (5.27) has at most one solution in even positive integers. Equation (5.27) has a solution in even positive integers only if $p \equiv 1$ or $5 \pmod 8$ and has a solution in odd positive integers only if $p \equiv A + 4 \pmod 8$. Moreover, equation (5.27) has a solution only if $\left(\frac{-A}{p}\right) = 1$.

Lemma 3.0.3 implies that equation (5.28) has at most one positive solution. If equation (5.28) has a solution, then u is odd and depending on the parity of v, $A \equiv 7$ or $2p - 1 \pmod 8$ and $\left(\frac{-A}{p}\right) = 1$.
Then, we have the following.

If $A \equiv 1 \pmod 8$, then equation (5.25) has at most one solution in even positive integers, equation (5.26) has at most one positive solution only if $p \equiv 1$ or $7 \pmod 8$, equation (5.27) has at most one solution in even positive integers only when $p \equiv 1$ or $5 \pmod 8$, and at most one solution in odd positive integers only when $p \equiv 5 \pmod 8$, and equation (5.28) has at most one positive solution only when $p \equiv 1$ or $5 \pmod 8$.

If $A \equiv 3 \pmod 8$, then equation (5.25) has at most one solution in even positive integers, equation (5.26) has no solutions, equation (5.27) has at most one solution in even positive integers only when $p \equiv 1$ or $5 \pmod 8$ and at most one solution in odd positive integers only when $p \equiv 7 \pmod 8$, and equation (5.28) has no solutions.

If $A \equiv 5 \pmod 8$, then equation (5.25) has at most two positive solutions, equation (5.26) has no solutions, equation (5.27) has at most one solution in even positive integers only when $p \equiv 1$ or $5 \pmod 8$ and at most one solution in odd positive integers only when $p \equiv 1 \pmod 8$, and equation (5.28) has at most one positive solution only when $p \equiv 3$ or $7 \pmod 8$.

If $A \equiv 7 \pmod 8$, then equation (5.25) has at most one solution in even positive integers, equation (5.26) has at most one positive solution only if $p \equiv 1$ or $7 \pmod 8$, equation (5.27) has at most one solution in even positive integers only when $p \equiv 1$ or $5 \pmod 8$ and at most one solution in odd positive integers only when $p \equiv 3 \pmod 8$, and equation (5.28) has at most one positive solution.

Moreover, equations (5.27) and (5.28) have solutions only if $\left(\frac{-A}{p}\right) = 1$. □

Chapter 6

Conclusion

The history of Cassels equation started with Cassel trying to find when the sum of three consecutive cubes equals a square. He reduced the problem to solving the Diophatine equation $y^2 = 3x(x^2 + 2)$. Luca and Walsh generalized the equation to $y^2 = nx(x^2 + 2)$ and found that this has at most $3(2^{\omega(n)-1})$ solutions where n is an integer. Chen got us closer to our Diophantine equations we studied here by supposing that $n = p$ an odd prime. He obtained that there are at most two positive integer solutions. It was Togbé who added the A when A is odd, and generalized it to $y^2 = px(Ax^2+2)$. He found at most seven poitive integer solutions. Li and Yuan changed this equation to $y^2 = px(Ax^2 - 2)$ and found five solutions. Finally Wu et al. considered $y^2 = px(Ax^2 - C),\ c \in \{\pm 1, \pm 4\}$. This equation has at most three positive integer solutions if $C = \pm 1$, at most seven positive integer solutions when $C = 4$, and at most eight positive integer solutions when $C = -4$

Now we have given the upper bounds for integral solutions of five more Diophantine equations. Before this paper we had the upperbounds on the number of integral solutions of the Diophantine equation $y^2 = px(Ax^2 + 2)$. We now have similar bounds set for $y^2 = px(Ax^2 \pm 1)$ as well as $y^2 = px(Ax^2 - 2)$ and finally $y^2 = px(Ax^2 \pm 4)$. A practical analogy to what we have done here is, when we come across these solutions, we now need to compute a Legendre symbol, and reduce A and p modulo 8. We quickly see how many solutions we expect to find. Before we had a maximum on these solutions. We knew how many we could expect to find at most, but now we have an greater view into when we have less. These proofs that we showed essentially work by factoring the Diophantine equation and showing that the results when applied to an assumption based on the Legendre symbol calculation and a reduction modulo 8 are resticted in the number of solutions the Diophantine equation can have.

A more technical way of describing our results, is to say we have found integral points on the elliptic curves $y^2 = px(Ax^2-C),\ C \in \pm 1, \pm 2, \pm 4$. Further work needs to be done to find the rational points to these same elliptic curves. This was not the aim of this paper and is an area of further research. More

research could be done on varying values of A and C. These values may have affect on the rank of these curves. It is very difficult to find elliptic curves with an arbitrary rank. The rank of an elliptic curve is of particular interest in the number theory as it is still an open question to find arbitrarily high ranking elliptic curves. It is conjectured that there is no maximum rank to elliptic curves. Currently the highest rank found on an elliptic curve is 28.

The very next area to do work in will be to find the rank of these equations when $A > 1$ is a square free integer and $C \in \{\pm 1, \pm 2, \pm 4\}$. We need this to see how these values affect the rank of the curve. To see when we have rank equal to zero and when we have a rank greater than zero with the values of A and C are the next steps.

References

[1] S. Akhtari, *The Diophantine equation $ax^4 - by^2 = 1$.*, J. Reine Angew. Math., 630 (2009), pp. 33–57.

[2] F. Bencherif, R.Boumahdi, T.Garici, and Z.Schedler, *Upper Bounds for the Number of Solutions for the Diophantine Equation $y^2 = px(Ax^2 - C)(C = 2, \pm 1, \pm 4)$* (2018)

[3] V. Bouniakowsky, *Note sur l'emploi des procédés élémentaires du Calcul Intégral dans des questions relatives a l'Analyse de Diophante.*, Bull. de St. Pétersb., 11 (1853), pp. 65–74.

[4] J. Cassels, *A Diophantine equation.*, Glasg. Math. J., 27 (1985), pp. 11–18.

[5] J. Chen and P. Voutier, *Complete solution of the diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equations.*, J. Number Theory, 62 (1997), pp. 71–99.

[6] L. Chen, *On the Diophantine equation $y^2 = px(x^2 + 2)$.*, Acta Math. Sin., Chin. Ser., 53 (2010), pp. 83–86.

[7] L. E. Dickson, *History of the Theory of Numbers*, vol. 256, Chelsea Pub. Co., 1952.

[8] T. Garici, O. Kihel, and J. Larone, *The number of solutions to $y^2 = px(Ax^2 + 2)$*, Publ. Inst. Math., Nouv. Sér., (to appear).

[9] A. Gérardin, *Solution de l'équation $x^3 + y^3 + z^3 = u^2$ (question 3129, de E. N. Barisien).* Interméd. des math. 23, 7–8, 1916.

[10] W. Ljunggren, *Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$.* 12. Skand. Mat.-Kongr., Lund 1953, 188-194 (1954)., 1954.

[11] W. Ljunggren, *On the Diophantine equation $Ax^4 - By^2 = C$ $(C = 1, 4)$.*, Math. Scand., 21 (1967), pp. 149–158.

[12] F. Luca and P. Walsh, *Squares in Lehmer Sequences and some Diophantine Applications*, Acta Arith., 100 (2001), pp. 47–62.

[13] F. Luca and P. Walsh, *On a Diophantine equation of Cassels.*, Glasg. Math. J., 47 (2005), pp. 303–307.

[14] J. Luo and P. Yuan, *Square-classes in Lehmer sequences having odd parameters and their applications.*, Acta Arith., 127 (2007), pp. 49–62.

[15] T. Nagell, *Introduction to number theory*, John Wiley & sons, Inc., New York, Stockholm (1951)

[16] A. Togbé, *A note on the Diophantine equation* $y^2 = px(Ax^2 + 2)$., Afr. Mat., 25 (2014), pp. 739–744.

[17] A. Togbém P.M Voutier, and P.G Walsh, *Solving a family of Thue equations with an application to the equation* $x^2 - dy^4 = 1$, Acta Arith., 120 (2005), pp. 39–58.

[18] A. Togbé and P. Yuan, *On a variant of a Diophantine equation of Cassels.*, Glas. Mat., III. Ser., 46 (2011), pp. 325–331.

[19] W. Wu, A. Togbé, B. He, and S. Yang, *On the number of solutions of the Diophantine equation* $y^2 = nx(Ax^2 \pm C)$, S. Pac. J. Pure Appl. Math., 2 (2013), pp. 1–16.

[20] P. Yuan, *Rational and algebraic approximations of algebraic numbers and their application.*, Sci. China, Ser. A, 40 (1997), pp. 1045–1051.

[21] P. Yuan and Y. Li, *On the Diophantine equation* $y^2 = px(Ax^2 - 2)$., JP J. Algebra Number Theory Appl., 14 (2009), pp. 185–190.

[22] ——, *Squares in Lehmer sequences and the Diophantine equation* $Ax^4 - By^2 = 2$., Acta Arith., 139 (2009), pp. 275–302.