UNLV University Libraries
University of Nevada, Las Vegas

UNLV Theses, Dissertations, Professional Papers, and Capstones

5-1-2015

A Comparison of Recent Results on the Unicity Conjecture of the Markoff Equation

Brandon John Metz
University of Nevada, Las Vegas, metzb513@gmail.com

Follow this and additional works at: https://digitalscholarship.unlv.edu/thesesdissertations

Part of the Mathematics Commons

Repository Citation

Metz, Brandon John, "A Comparison of Recent Results on the Unicity Conjecture of the Markoff Equation" (2015). *UNLV Theses, Dissertations, Professional Papers, and Capstones*. 2389.
https://digitalscholarship.unlv.edu/thesesdissertations/2389

This Thesis is protected by copyright and/or related rights. It has been brought to you by Digital Scholarship@UNLV with permission from the rights-holder(s). You are free to use this Thesis in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/or on the work itself.

This Thesis has been accepted for inclusion in UNLV Theses, Dissertations, Professional Papers, and Capstones by an authorized administrator of Digital Scholarship@UNLV. For more information, please contact digitalscholarship@unlv.edu.

A COMPARISON OF RESULTS ON THE UNICITY CONJECTURE OF THE MARKOFF EQUATION

by

Brandon John Metz

Bachelor of Science in Mathematics
Elizabethtown College
2009

A thesis submitted in partial fulfillment
of the requirements for the

Master of Science - Mathematical Science
Department of Mathematical Sciences
College of Sciences

The Graduate College
University of Nevada, Las Vegas
May 2015

Copyright by Brandon Metz, 2015

All Rights Reserved

UNLV | GRADUATE COLLEGE

We recommend the thesis prepared under our supervision by

Brandon John Metz

entitled

A Comparison of Recent Results on the Unicity Conjecture of the Markoff Equation

is approved in partial fulfillment of the requirements for the degree of

Master of Science - Mathematical Sciences

Department of Mathematical Sciences

Arthur Baragar, Ph.D., Committee Chair

Ebrahim Salehi, Ph.D., Committee Member

Peter Shiue, Ph.D., Committee Member

Stephen Miller, Ph.D., Graduate College Representative

Kathryn Hausbeck Korgan, Ph.D., Interim Dean of the Graduate College

May 2015

ABSTRACT

In this thesis we discuss the positive integer solutions to the equation known as the Markoff equation

$$x^2 + y^2 + z^2 = 3xyz.$$

Each solution to the equation is a permutation of a triple (x, y, z) with $0 \leq x \leq y \leq z$, which is called a *Markoff triple* and each integer of the triple is referred to as a *Markoff number.*

In 1913, Fröbenius conjectured that given an ordered Markoff triple (x, y, z), then both x and y are uniquely determined by z. In other words, if both (x_1, y_1, z) and (x_2, y_2, z) are solutions to the Markoff equation with $x_i \leq y_i \leq z$, then $x_1 = x_2$ and $y_1 = y_2$. When this is true for a particular z, we say that z is unique. Since the time of Fröbenius there have been numerous results on what we refer to now as the Fröbenius Conjecture.

In 1996 Baragar proved that given a Markoff number z, it is unique whenever z, $3z - 2$, or $3z + 2$ is a prime, twice a prime or four times a prime. In 2001, Button proved that z is unique whenever $z = p^r$, where p is prime and also when $z = kp^r$ for p prime and $k < \sqrt[4]{z}$. In 2012, Chen proved the conjecture holds when $3z \pm 2 = kp^r$ for p prime and $k < \sqrt[14]{3z \pm 2}$. There is a recent result due to Srinivasan that utilizes divisors of the discriminant of quadratic forms, the details of which will be explained in the thesis.

The goal of this thesis is to empirically investigate how "good" these results are, in the sense that we wish to know how many Markoff triples are shown to be unique with each successive result. In Baragar's paper from 1996, it was shown that all Markoff triples with $z < 10^{140}$ are unique, and that approximately 6% of them satisfied the conditions of his main result. Due to the results from Button (2001) and Chen (2012), roughly 60% of all Markoff triples with $z < 10^{140}$ are proven to be unique. This is accomplished by writing computer algorithms to test each result.

ACKNOWLEDGEMENTS

I would like to thank my family and friends for all of their support. Special thanks goes to my fiancée Dawn Sturgeon, for without her this would have been impossible.

TABLE OF CONTENTS

ABSTRACT iii

ACKNOWLEDGEMENTS v

LIST OF FIGURES vii

CHAPTER 1. INTRODUCTION AND RESULTS 1

1.1. INTRODUCTION 1

1.2. RESULTS 4

CHAPTER 2. METHODS 8

CHAPTER 3. HISTORY AND BACKGROUND OF THE MARKOFF EQUATION 24

CHAPTER 4. ELEMENTARY METHODS 36

BIBLIOGRAPHY 40

CURRICULUM VITAE 41

LIST OF FIGURES

Figure 1.1 2

Figure 1.2 7

CHAPTER 1

INTRODUCTION AND RESULTS

1. INTRODUCTION

The Markoff equation has been studied by many famous mathematicians for over 100 years. It was discovered early, that all the positive solutions to the Markoff equation could be generated from just a single solution $(1, 1, 1)$, which is called the *fundamental solution*. Suppose that (x, y, z) is a solution to the Markoff equation. Then it is easy to verify through substitution that the following are also solutions:

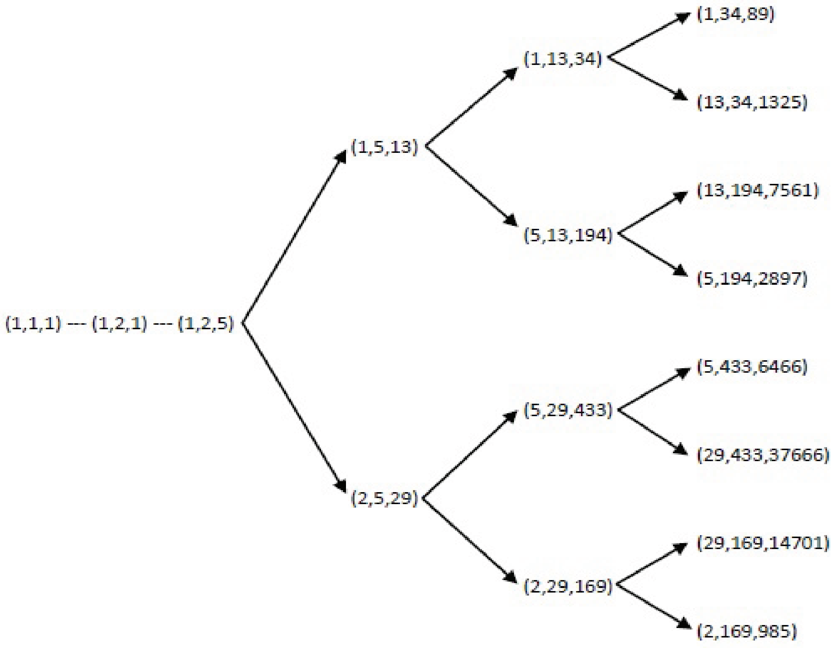
$$(x, y, 3xy - z)$$
$$(x, z, 3xz - y)$$
$$(y, z, 3yz - x)$$

If $x \leq y \leq z$, then the first triple is will not yield a triple with a greater maximal element, whereas the other two will. Consider a solution (x, y, z) under the following transformations:

$$\phi : (x, y, z) \longmapsto (x, z, 3xz - y)$$
$$\psi : (x, y, z) \longmapsto (y, z, 3yz - x)$$

All positive solutions of the Markoff equation can be generated from the fundamental solution $(1, 1, 1)$ and these two transformations. In fact, these two transformations generate a binary tree, where the top branch is given by ϕ and the bottom branch is given by ψ. We call this tree the *Markoff Tree*. The figure below explains the branching process.

FIGURE 1.1



With the introduction of the Markoff Tree, the uniqueness condition could be summarized as,"A Markoff number is unique if it occurs exactly once as the largest component of a Markoff triple in the Markoff Tree".

This branching concept is quite useful as it allows us to quickly create a list of Markoff numbers. We can write a computer algorithm that emulates this branching process in order to generate all 18,906 Markoff Numbers below 10^{140} in only a few minutes.

The code in this thesis is written primarily in Python. The initial programs are fairly simple and do not require more than basic arithmetic. However, as we progress through the results, we are forced to use more advanced functions. One of the main issues we will encounter is primality testing, since it will be necessary for us to test whether certain numbers are prime. Specifically, the results due to Baragar, Button, and Chen all revolve around prime numbers.

At that time we will switch to SAGE, which is an open-source mathematical computing software suite utilizing the Python programming language. It includes numerous packages such as NumPy, SciPy, and matplotlib. Included in the mathematical packages are modules and functions used for primality testing and factoring of integers, the latter of which will be quite handy when trying to test Srinivasan's result. For readers who may not be familiar with Python, semi-colons and braces are not used to indicate statements and bodies of code as they do in other programming languages. Python alleviates the need to use these symbols by keeping track of space and indentation. For example, in `C++`, if we want to write a for-loop to print out the first 10 positive integers it would look something like this:

```
for(int i = 1; i < 11; i++)
{
   cout << i;
}
```

Note that although this code has indentation, it is merely common practice to indent for easier reading even if it has no effect on the code. We could just as easily have written this code in a single line.

```
for(int = 1; i < 11; i++){cout << i}
```

However, this is not optimal when the body of a loop contains more than one command. In Python, the same script would be written this way:

```
for i in range(1,11):
   print i
```

Python requires indentation in order for it to know if a line of code is connected to the previous line. This is just an example for the reader to keep in mind whilst reading through the code given throughout this thesis.

2. RESULTS

The goal of this thesis is to ascertain the usefulness of the other theorems. Due to time constraints and hardware, only the first 6,000 Markoff numbers are considered for many of the theorems.

In [**2**], Baragar mentions that among all Markoff numbers below 10^{140}, roughly 6% of them satisfy the conditions of the following theorem.

Theorem 1 (Baragar 1996). *If either m, $3m-2$, or $3m+2$ is a prime, twice a prime, or four times a prime, then there exists at most one integer pair (x, y) so that (x, y, m) is a Markoff triple.*

The first theorem that we look at will be the main theorem from Button[**4**], which is given here:

Theorem 2 (Button 2001). *If (x, y, m) is an integer solution to the Markoff equation, then m is unique if $m = kp^r$, where p is prime and $k^4 < m$.*

The reader will notice that the algorithm used for Theorem 2 in Chapter 2 only tests for solutions of the form $m = kp$. The reason for this is that when the code is changed to check for solutions of the form $m = kp^r$, only one solution in the first 6,000 Markoff numbers satisfied found. This seems at first glance, to be deceptive, since one might expect the extension to powers of p to be significant. On the other hand, the number of solutions of the form $m = kp$ is quite significant. In the first 6,000 Markoff numbers, roughly 37% satisfy the conditions of Theorem 2, whereas almost 12% satisfy the conditions of Theorem 1. This theorem captures many more solutions and most certainly has some substance to it. The next theorem, due to F. Chen and Y. Chen[**5**], can be thought of as a completion of Button's result.

THEOREM 3 (Chen 2013). *If (x, y, m) is an integer solution to the Markoff equation, then m is unique if $3m - 2 = kp^r$ or $3m + 2 = kp^r$, where $k < \sqrt[14]{3m-2}$ or $\sqrt[14]{3m+2}$ respectively.*

In the first 6,000 Markoff numbers, roughly 20% satisfy the conditions of Theorem 3. The reader should note that although these solutions satisfy the conditions of Theorem 3, many of those also satisfy Theorems 1 and 2 as well. In fact, only 9% of the first 6,000 Markoff numbers satisfy only theorem 3. Although not as large of a gain as Button's, it is significant. The last theorem that we cover is due to Srinivisan[**7**].

THEOREM 4 (Srinivasan 2009). *Let m be an odd Markoff number and $d = 9m^2 - 4$. Assume that for every $0 < d_1 < \sqrt{d}$ with $d = d_1 d_2$, $d_1 \nmid 3m - 2$ and $gcd(d_1, d_2) = 1$, one of the following is true.*

(1) There exists a prime $r \mid d_1$ such that $(\frac{d_2}{r}) = -1$.

(2) There exists a prime $r \mid d_2$ such that $(\frac{d_1}{r}) = -1$.

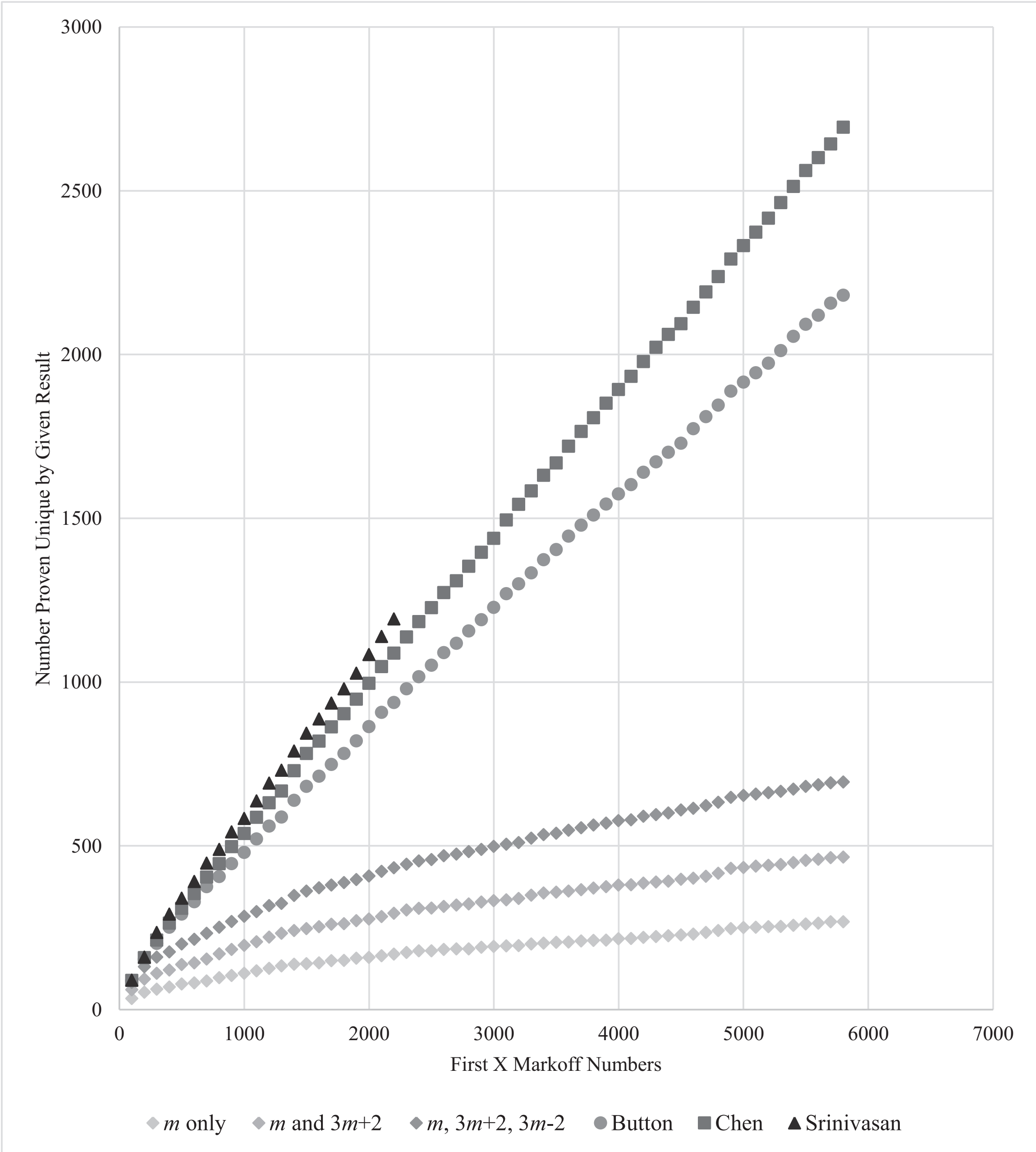
Then m is unique.

This theorem requires us to factor the discriminant and examine each divisor in turn. Since factoring is a computationally intensive task, only the first 2,200 Markoff numbers are considered for theorem 4. In the first 2,200 Markoff numbers roughly 13% satisfy the conditions of Srinivasan's theorem. However, most of them also satisfy the conditions of the other theorems. In fact in the first 2,200 Markoff numbers, only 65 were unique, which is just under 3%. In other words, in the first few thousand Markoff numbers, this theorem is not much of an improvement over the other ones.

Listed below is a graph representing the number of unique Markoff numbers which can be shown to be unique by the previous theorems. Each new line represents adding another theorem into the mix. For example, the line labeled as Button, shows the total number of Markoff numbers which satisfy the conditions of either Baragar's theorem or Button's theorem. Graphing the results of the tests in this way will give us an idea of how many more Markoff numbers are "captured" by each successive theorem.

We can see that with the addition of Button's theorem and Chens' theorem, there is quite a large increase of new Markoff numbers being "captured". Whereas, very few new Markoff numbers are captured by the addition of Srinivasan's theorem.

Figure 1.2



3000
2500
2000
1500
1000
500
0
0
1000
2000
3000
4000
5000
6000
7000
Number Proven Unique by Given Result
First X Markoff Numbers
m only
m and 3m+2
m, 3m+2, 3m-2
Button
Chen
Srinivasan

CHAPTER 2

METHODS

The first step in setting out to test these theorems is to obtain a list of all the Markoff numbers below 10^{140}. In [**2**], Baragar found 18,906 Markoff numbers below 10^{140}, and determined that 1197 of them fall under the conditions of his theorem. This set of solutions will be used as input for each test. It would be very slow to run a for loop to print out the values that satisfy the Markoff equation, so instead we use a recursive function to generate the solutions and print them to a file for later use. Since the values are being written to a file instead of being stored, the program executes at a much faster pace.

Recall that all the positive solutions to the Markoff equation can be generated from a single solution $(1, 1, 1)$ using the following transformations:

$$(x, y, z) \longmapsto (x, z, 3xz - y) \text{ and } (x, y, z) \longmapsto (y, z, 3yz - x)$$

The first generates the top branch while the second one generates the bottom branch at each node of the Markoff Tree. This concept is what we will use to generate all the solutions below 10^{140}, the code for the main function of the script is given below.

```
def go(list_, i, T):
   if list_[2] < (10**T):
      f = open('solutions','a+')
      f.write("%r\n % list_[2]))
      f.close()
```

```
        go(top_(list_), i, T)
        go(bottom_(list_), i, T)
        i = i + 1
    else:
        return list_
```

The first thing we should take note of in this section are the variables being passed to the function. The first variable, `list_`, is an array representing an ordered triple (x_0, x_1, x_2). The second variable `i` is used here to keep a tally of how many total solutions have been found. In Python, variables defined outside of a function are not automatically categorized as global variables, which would be more useful to use than to simply keep passing the variable `i` to the function each time. The same thing could be said about the next variable `T`, which is the exponent of 10^T, which is used to stop the function from calling itself indefinitely.

Each time the function `go` is called, it first checks whether the z component of the triple passed to it is less than 10^{140}. If the z component is below the bound, the function opens the *Solutions.txt* file in writing mode and writes to it the current value of the `list_[2]` and then immediately closes the file. The next two lines of code both call the `go` function, each with a different input. The line `go(top_(list_),i,T)` calls the `go` function using `top_(list_)` which takes the current value of `list_` and returns the next Markoff triple using the transformation,

$$(x, y, z) \longmapsto (x, z, 3xz - y)$$

The code for this transformation is given by:

```
def top_(list_):
```

```
    return [list_[0],list_[2],3*list_[0]*list_[2]-list_[1]]
```

The second line, `go(bottom_(list_),i,T)` calls the `go` function using the value of `bottom_(list_)` which returns the next Markoff triple using the transformation,

$$(x, y, z) \longmapsto (y, z, 3yz - x)$$

which is represented by the code,

```
def bottom_(list_):
    return [list_[1],list_[2],3*list_[1]*list_[2]-list_[0]]
```

The `go` function will continue to call itself until the `list_[2]` is no longer less than 10^{140}. In this way, the function will go through all the triples in the topmost branch of the Markoff Tree until it reaches a triple whose z component is too large. Then it will print the bottom branch of that same node. The end result will be a list of Markoff numbers which are less than 10^{140}.

In terms of running time, this script is quite fast, taking nine minutes to find, write to a file, and count all Markoff numbers below 10^{140}. In [**2**], Baragar mentioned that at the time of his 1996 paper, the same calculation took about ten hours of computing time. Although the previous script will give us a list of Markoff numbers, they are not in numerical order. We use a simple script to sort the values in the file. With the solutions sorted, the next step is to write code that will check how many fall under the conditions of Baragar's results.

Once we have sorted the output we can write scripts to test Baragar's results. This brings us to the first theorem.

THEOREM 1 (Baragar). *If either m, $3m-2$, or $3m+2$ is a prime, twice a prime, or four times a prime, then there exists at most one integer pair (x, y) so that (x, y, m) is a Markoff triple.*

This theorem is one of the more elegant theorems, due in most part to the simplicity of the theorem's statement. Not only is it simply stated, but it is obvious how we should write a script to test it. Since we need to be able to test whether a number is prime or not, as mentioned previously, We need to switch from base packages to the more advanced libraries available to python programmers. We will need to test each possible outcome from the theorem ($m = p$, $m = 2p$, etc.), and we do this by combining all of the possible tests into a single script.

```
from sage.all import*
f = open("Sorted Solutions.txt ",'r')
count = 0
prime_count = 0
twice_a_prime = 0
3m_plus_two_prime = 0
3m_plus_two_twice_a_prime = 0
3m_plus_two_four_a_prime =  0
3m_minus_two_prime = 0
3m_minus_two_twice_a_prime = 0
3m_minus_two_four_a_prime = 0
for line in f:
   num = long(line[:len(line)-2])
```

```
3m_plus_two = 3 * num + 2
3m_minus_two = 3 * num - 2
if is_prime(num) == True:
   prime_count+= 1
if num % 2 ==0 and is_prime(num/2) == True:
   twice_a_prime += 1
if is_prime(3m_plus_two) == True:
   3m_plus_two_prime += 1
if 3m_plus_two % 2 == 0 and is_prime(3m_plus_two/2) == True:
   3m_plus_two_twice_a_prime += 1
if 3m_plus_two % 4 == 0 and is_prime(3m_plus_two/4) == True:
   3m_plus_two_four_a_prime += 1
if is_prime(3m_minus_two) == True:
   3m_minus_two_prime += 1
if 3m_minus_two % 2 == 0 and is_prime(3m_minus_two/2) == True:
   3m_minus_two_twice_a_prime += 1
if 3m_minus_two % 4 == 0 and is_prime(3m_minus_two/4) == True:
   3m_minus_two_four_a_prime += 1
count += 1
print "We have checked %r many solutions." % count
f.close()
```

The reader will have noticed the % symbol in the code above. This is the modulus symbol, for use in modular arithmetic. The variables at the beginning of the code are pretty self-explanatory, except for maybe `count`, which just keeps track of how many Markoff numbers have been checked so far. The others simply keep track of how many fall into each category. The next block of code uses a for-loop to run through the *Sorted Solutions.txt* file.

```
for line in f:
    num = long(line[:len(line)-2])
    3m_plus_two = 3 * num + 2
    3m_minus_two = 3 * num - 2
```

The numbers stored in *Sorted Solutions.txt* are each on their own line, and the for-loop in the code will iterate over each line. Therefore, the variable `line` will assume the value of each number as the for-loop continues. The numbers stored in file are stored as strings, so they must first be converted to integers for them to be of any use. The following line of code will take the string from the current line in the file, and then convert it into an integer:

```
num = long(line[:len(line)-2])
```

Once each string has been converted to an integer, the variables `three_m_plus_two` and `three_m_minus_two` are defined in the next two lines of code. At this point, there are variables each representing $z, 3z+2$, and $3z-2$, and the next step is to test whether each one is prime, twice a prime, or four times a prime. The following code was used to actually perform the testing, for each value of `num`:

```
    if is_prime(num) == True:
        prime_count+= 1
    if num % 2 == 0 and is_prime(num/2) == True:
```

```
        twice_a_prime += 1
    if is_prime(3m_plus_two) == True:
        3m_plus_two_prime += 1
    if 3m_plus_two % 2 == 0 and is_prime(3m_plus_two/2) == True:
        3m_plus_two_twice_a_prime += 1
    if 3m_plus_two % 4 == 0 and is_prime(3m_plus_two/4) == True:
        3m_plus_two_four_a_prime += 1
    if is_prime(3m_minus_two) == True:
        3m_minus_two_prime += 1
    if 3m_minus_two % 2 == 0 and is_prime(3m_minus_two/2) == True:
        3m_minus_two_twice_a_prime += 1
    if 3m_minus_two % 4 == 0 and is_prime(3m_minus_two/4) == True:
        3m_minus_two_four_a_prime += 1
    count += 1
```

The `is_prime` function will return `True` if the input is prime and `False` otherwise, as one might expect. The first `if` statement will test whether the number is prime. The second `if` statement first checks whether the number is divisible by two (i.e. congruent to 0 modulo 2) and whether its half is prime. If so, then `num` is twice a prime, and the script increments corresponding variable by one. The remaining `if` statements all follow the same format. They first test whether the variable is prime, twice, or four times a prime by using `% 2 == 0` or `% 4 == 0`. Then they test whether the variable itself is prime, or the variable divided by two or four is prime, respectively.

The next order of business is to check for solutions which satisfy the criteria of Button's result, which is summarized by the following theorem.

THEOREM 2 (Button). *If (x, y, m) is an integer solution to the Markoff equation, then m is unique if $m = kp^r$, where p is prime and $k^4 < m$.*

Since all the Markoff numbers below 10^{140} have been verified as unique, we can use this to our advantage in order to test the effectiveness of this theorem as well as the others. In the case of theorem 2, we know that m will be unique as long as $k < 10^{35}$. When we get to theorem 3 our bound for will change to $k < 10^{10}$, in order to stay below 10^{140}.

Until this theorem, the only thing that we needed to be able to do was tell whether an integer was prime. This theorem requires us to factor the Markoff number m, which is much more computationally intensive than primality testing. Fortunately, SAGE has built in functions for factoring integers, specifically, the `factor()` function. This function is not limited to factoring integers, but that is all that is needed here. Suppose we were to factor the integer 126. Then `factor(126)` would return the output `2 * 3^2 * 7`. However, this is not a string, but a SAGE object and is simply what is returned by the function and is not easily used in code.

The instance `factor(126)` of the Factorization class, is not itself an array, but it does contain an array that represents the factorization of its input for easy use. Consider the following `for` loop,

```
for x in factor(126):
    print x
```

which will return the following output,

```
(2,1)
(3,2)
(7,1).
```

Each tuple that was printed out is of the form (p_i, e_i) where $\prod p_i^{e_i} = 126$. Further, the elements of each tuple can be accessed in code exactly as one would access elements of an array. For example,

```
factor(126)[0] = (2,1)
factor(126)[0][0] = 2
factor(126)[0][1] = 1.
```

This enables the user to find, store, and use each factor of the integer. This is what will be used for Button's theorem. Below is the code,

```
if factor(num)[len(factor(num))-1][0]**factor(num)[len(factor(num))-1][1]
    >= (num ** float(3.0/4)):
```

Although it is a single line of code, there is quite a bit happening here. The first thing to observe is

```
factor(num)[len(factor(num))-1][0].
```

Recall that the variable `num` will assume the value of each Markoff number below 10^{140}, so it is necessary that the code will work for any integer, no matter how large. If `num` $= \prod p_i^{e_i}$, then `factor(num)` will contain the array `[(`p_1`,`e_1`), (`p_2`,`e_2`), ...,(`p_n`,`e_n`)]`, which is an array of length n. However the element `factor(num)[n]` will return an error since it is outside the index range, so it must be offset by 1 in order to ensure that the last tuple is referenced without error, which yields the segment of code above. That is, to access the last prime factor, the index `len(factor(num))-1` is used and `factor(num)[len(factor(num))-1] = `(p_n, e_n). It is straightforward to see that the entire segment of code above will represent the value of p_n. The second segment,

```
factor(num)[len(factor(num))-1][1].
```

represents the exponent e_n, and the `**` operator is the operation of exponentiation. Therefore, the initial segment of the code represents the largest prime(power) factor of the variable `num`. Instead of taking the product of the remaining factors to form k, which would increase computing time, we instead use the largest prime(power) factor and test whether it is greater than the cube of the fourth root of `num`. That is, if $k < \sqrt[4]{m}$, then $\frac{m}{k} = p_n^{e_n} \geq \sqrt[4]{m^3}$. Testing $p_n^{e_n}$ will cut down on the computing time and is just as valid. The last part of the code is where this is done.

```
(num ** float(3.0/4))
```

With the completion of this algorithm, we can now set our sights on Chens' theorem.

THEOREM 3 (Chen). *If (x, y, z) is an integer solution to the Markoff equation, then m is unique if $3m-2 = kp^r$ or $3m+2 = kp^r$, where $k < \sqrt[14]{3m-2}$ or $\sqrt[14]{3m+2}$ respectively.*

The first thing to note, is that the bound on k is different. In this case we need $k < \sqrt[14]{3m \pm 2}$. The code for testing this is almost exactly the same as the code we used for Button's result, with that slight modification. The code is as follows:

```
kay = m_plus

if m_plus != 1:
```

```
    kay = kay / (factor(m_plus)[len(factor(m_plus))-1][0]
        **factor(m_plus)[len(factor(m_plus))-1][1])
    if kay < m_plus ** float(1.0/14):
        3m_plus_two_kp += 1
kay = m_minus
if m_minus != 1:
    kay = kay / (factor(m_minus)[len(factor(m_minus))-1][0]
        **factor(m_minus)[len(factor(m_minus))-1][1])
    if kay < m_minus ** float(1.0/14):
        3m_minus_two_kp += 1
```

The variables `m_plus` and `m_minus` represent the value of $3m + 2$ and $3m - 2$, respectively. The case where $3m - 2 = 1$ is handled separately, since the `factor()` function does not treat 1 the same as other integers. Recall that an instance of the Factorization class contains an array with all the factors of the given input.

```
    kay = kay / (factor(m_minus)[len(factor(m_minus))-1][0]
        **factor(m_minus)[len(factor(m_minus))-1][1])
```

This segment of the code takes `kay`, which is equal to $3m \pm 2$, and divides it by the largest prime power factor of $3m \pm 2$. This factors $3m \pm 2$ into kp^r as desired. Once k has been determined a simple comparison test is used.

```
    if kay < m_plus ** float(1.0/14):
        3m_plus_two_kp += 1
```

Up until this point, the theorems mentioned were all quite straightforward, and easy to digest. The next theorem requires a little more effort.

Theorem 4 (Srinivasan). *Let m be an odd Markoff number and $d = 9m^2 - 4$. Assume that for every $0 < d_1 < \sqrt{d}$ with $d = d_1 d_2$, $d_1 \nmid 3m - 2$ and $gcd(d_1,d_2) = 1$, one of the following is true.*

(1) There exists a prime $r \mid d_1$ such that $(\frac{d_2}{r}) = -1$.

(2) There exists a prime $r \mid d_2$ such that $(\frac{d_1}{r}) = -1$.

Then m is unique.

Note that in condition (1), the Jacobi symbol is used with d_2 and a prime $r \mid d_1$, and vice versa in condition (2). This means that for every d_1 dividing the discriminant d, we must test $(\frac{d_2}{r})$ for each prime r dividing d_1. The same must be done for d_2 as well. The first thing that we must do is define functions which will test conditions (1) and (2) above. The functions are given below.

```
def condition1(*args):
   for prime in factor(d_1):
      if kronecker_symbol(d_2, prime[0]) == -1:
         return True
      else:
         return False
def condition2(*args):
   for prime in factor(d_2):
      if kronecker_symbol(d_1, prime[0]) == -1:
         return True
      else:
         return False
```

The two functions are quite similar, as you would expect. Observe that each function is passed the `*args` argument. We use this when we are not certain of how many arguments to pass to the function. In other words, the functions will accept any number of variables when called. A new SAGE function is introduced here, the `kronecker_symbol()` function. Note that in condition (1) and (2) of Srinivasan's theorem, the Jacobi symbols $(\frac{d_2}{r})$ and $(\frac{d_1}{r})$, are used. As was mentioned previously, the Jacobi symbol is a generalization of the Legendre symbol with a nonnegative integer modulus. The Kronecker symbol is simply a generalization of the Jacobi symbol to all integers.

The rest of the code will determine what values to use for d_1 and d_2, and finally, to determine whether or not a Markoff number satisfies the conditions of the theorem. The remaining code is given here below.

```
unique_count = 0
count = 0
for num in f:
   c = long(num)
   d= 9*c**2 -4
   list_ = []
   for num in divisors(d):
      if num < math.sqrt(d) and (3*c-2) % num != 0:
         list_ += [num]
   pass_count = 0
   fail_count = 0
```

```
    for d_1 in list_:
        d_2 = d / d_1
        if condition1(d_1, d_2) == True or condition2(d_1,d_2) == True:
            pass_count += 1
        else:
            fail_count += 1
            break
    if pass_count == len(list_) and len(list_) != 0:
        g.write("%r \n" % c)
        unique_count += 1
    count += 1
    if count % 100 == 0:
        print "There are %r many unique markoff numbers below %r"
             %(unique_count, count)
        g.write( "-*70 +  "\n")
```

The variable `unique_count` is a running total of all the Markoff numbers that satisfy the theorem's conditions, whereas `count` is just a total of how many solutions we have checked. The first `for`-loop at the beginning is the standard one used to pull each number from the input text. The loop begins by setting `d = 9*c**2 - 4`. Consider the next segment of code, the second `for`-loop.

```
for num in divisors(d):
    if num < math.sqrt(d) and (3*c-2) % num != 0:
        list_ += [num]
```

This segment of code is what we use to determine which divisors of the discriminant d are going to be tested. The `divisors(n)` function accepts an integer as input and returns an array of all the integer divisors of `n`. In this way the loop then tests whether each divisor of d satisfies the assumptions of the theorem. If one of the divisors does pass this initial test, it is then added to the `list_` array to be used later. Once the candidates for d_1 have been determined, the variables `pass_count` and `fail_count` are initialized, and will count how many d_1's pass or fail the test.

It is important to keep in mind that in Srinivasan's theorem, every possible d_1 must pass condition (1) or (2). That is for every pair of d_1 and d_2, there exists either a prime r dividing d_1 such that $(\frac{d_2}{r}) = -1$ or a prime r dividing d_2 such that $(\frac{d_1}{r}) = -1$. So if there is even one pair of d_1 and d_2 that fails both condition (1) and (2), then the given Markoff number fails Srinivasan's test. This is the motivation for the next segment of code.

```
for d_1 in list_:
    d_2 = d / d_1
    if condition1(d_1, d_2) == True or condition2(d_1,d_2) == True:
        pass_count += 1
    else:
        fail_count += 1
        break
if pass_count == len(list_) and len(list_) != 0:
    unique_count += 1
```

This `for`-loop takes each d_1 from the `list_` array and tests whether the pair of d_1 and d_2 satisfy either condition (1) or (2). If so, then `pass_count` is incremented by 1. If not, then `fail_count` is incremented by 1 and the `for`-loop immediately ends, due to the `break` command. By escaping the `for`-loop upon a failure, computing time is diminished, since there is no point in continuing once a failure has been found. The variable `pass_count` is the number d_1's that pass condition (1) or (2). A Markoff number passes Srinivasan's test if every possible d_1 passes the conditions. Therefore, if the number of passes is the same as the number of d_1's, then the given Markoff number passes the test. This is seen in the `if` statement above.

It should not surprise the reader to learn that this script runs incredibly slow. This theorem requires us to factor the discriminant and examine each divisor in turn. For this reason alone, we consider only the first 2,200 Markoff numbers.

CHAPTER 3

HISTORY AND BACKGROUND OF THE MARKOFF EQUATION

One of the most common problems in mathematics is the approximation of irrational numbers. One might start by asking, given an irrational number, is it possible to find a rational number arbitrarily close to it? Anyone familiar with analysis will say that this is trivial. Given any irrational number α, there exists a rational number r such that,

$$|\alpha - r| < \epsilon$$

for any $\epsilon > 0$. It is well-known that every irrational number is the limit of some sequence of rational numbers. However, the terms of such sequences tend to have very large denominators, making them tedious to work with and computationally cumbersome. This introduces a new question, similar to the first one. Is it possible to find a rational number close to the number α, whose denominator is relatively small? An answer to this was provided by Dirichlet.

Theorem 5 (Dirichlet 1837). *Let $\alpha \in \mathbb{R}$ and $N \in \mathbb{N}$. Then there exists a rational number $\frac{p}{q}$ with $q \leq N$ such that,*

$$|\alpha - \tfrac{p}{q}| < \tfrac{1}{qN}.$$

This theorem of Dirichlet first placed a bound on the denominator. The following corollary provides an even stronger result.

Corollary 6. *Let α be an irrational number. Then there are infinitely many rational numbers $\frac{p}{q}$ such that*

$$|\alpha - \tfrac{p}{q}| < \tfrac{1}{q^2}$$

Although not a direct corollary to Dirichlet's theorem, the following proposition is also relevant.

Proposition 7. *If $\alpha \in \mathbb{Q}$, then for each $C > 0$, there exists only finitely many values $\frac{p}{q} \in \mathbb{Q}$ such that*

$$|\alpha - \tfrac{p}{q}| < \tfrac{C}{q^2}.$$

This corollary provides a way for checking whether or not a real number is rational. For if there are not infinitely many $\frac{p}{q}$ satisfying the first inequality, then α must not be irrational. Before continuing we define the order of approximation. We say that a real number α can be *approximated to order t* if there exists a constant $C_\alpha \in \mathbb{R}$ and infinitely many rational numbers $\frac{p}{q}$ such that

$$|\alpha - \tfrac{p}{q}| < \tfrac{C_\alpha}{q^t}$$

From the corollary we can see that if α is irrational, then it can be approximated to order of at least 2. The previous results only dealt with rational and irrational numbers, but what about the algebraic numbers? The following theorem due to Liouville provides some insight.

Theorem 8 (Liouville 1844). *Let α be irrational and algebraic of degree d. Then there exists a $C > 0$ such that for every $\frac{p}{q} \in \mathbb{Q}$,*

$$\tfrac{C}{q^d} < |\alpha - \tfrac{p}{q}|.$$

This theorem provides a bound for algebraic numbers, but its corollary is much more interesting.

Corollary 9. *An algebraic number of degree d can be approximated to order at most d.*

One can see how this corollary is quite useful. Recall that if α is the root of a non-zero polynomial d of finite degree in $\mathbb{Z}[x]$, we say that α is an *algebraic number*. Every rational number is algebraic of degree 1, and every algebraic irrational number is algebraic of degree greater than 1. However, not every real number is algebraic, for instance, the numbers π and e are both irrational. A real number which is not the root of some polynomial in $\mathbb{Z}[x]$ with finite degree, is called *transcendental*. From the previous corollary we obtain an interesting categorization of real numbers. Specifically, if a real number α can be approximated to order greater than 1, it is irrational. Furthermore, if it can be approximated to every order k, then it must be transcendental. Roth later showed that $\frac{1}{q^2}$ is the best possible bound for $|\alpha - \frac{p}{q}|$ for infinitely many $\frac{p}{q}$. However, this does not mean that the constant 1 is the best possible constant. Consider the inequality,

$$|\alpha - \tfrac{p}{q}| < \tfrac{1}{xq^2}.$$

Consider the set of all positive real numbers x that satisfy the inequality for infinitely many rational numbers $\frac{p}{q}$. We define L_α to be the supremum of this set, also called the *Lagrange number* of α.

Definition 1. The Lagrange Spectrum L, is the set of all possible L_α's for all real numbers α. That is, $L = \{L_\alpha : \alpha \in \mathbb{R}\}$.

At this point the reader may wonder what this has to do with the Markoff equation. It is not quite obvious how this is important. It turns out that what is referred to as $L_{<3} = \{L_\alpha \in L : L_\alpha < 3\}$, the portion of the Lagrange Spectrum that is below 3, has a direct connection with the set of Markoff numbers.

Consider the equation,

$$x^2 + y^2 + z^2 = 3xyz$$

which is more commonly known as the *Markoff Equation.* The solutions to this equation are integer triples (x, y, z), also called *Markoff Triples*, and each integer of the triple is a *Markoff number.* From here on the set of all Markoff numbers will be denoted by $\mathcal{M}$. The relation of the set $\mathcal{M}$ to the Lagrange Spectrum is seen in this theorem, due to Markoff.

THEOREM 10 (Markoff 1879). *There exist a sequence $\{\gamma_m\}$ of irrational numbers with*

$$\gamma_m = \tfrac{a_m + \sqrt{9m^2-4}}{b_m},\ m \in \mathcal{M}$$

with integers a_m and b_m, so that $L_{\gamma_m} < 3$. Specifically, the Lagrange Spectrum below 3 can be written in the form,

$$L_{<3} = \{\tfrac{\sqrt{9m^2-4}}{m} : m \in \mathcal{M}\}$$

Markoff himself was not directly interested in the Lagrange Spectrum, but in quadratic forms. In order to see where this theorem comes from, some information on quadratic forms is necessary. The reader should be aware that Markoff's theorem was sufficiently complex that Enrico Bombieri published his own proof of the theorem in [**3**].

Definition 2. A function of the form $f(x, y) = ax^2 + bxy + cy^2$, with $a, b, c \in \mathbb{R}$, is called a *quadratic form*. The *discriminant* of a quadratic form f is denoted by $\Delta = b^2 - 4ac$. A quadratic form is said to be *definite* if $\Delta < 0$ and *indefinite* if $\Delta > 0$.

Let f be an indefinite quadratic form. The following definitions will be important:

Definition 3. Let f be an indefinite quadratic form. The *uniform arithmetic minimum* of the form f is given by,

$$m(f) = \inf\{|f(x, y)| : f(x, y) \neq 0, x, y \in \mathbb{Z}\}$$

and the *Markoff value* for the form f is given by,

$$M(f) = \tfrac{\sqrt{\Delta}}{m(f)}.$$

The *Markoff Spectrum* is the collection of all the Markoff values $M(f)$ over the set of all indefinite forms. We will denote the Markoff Spectrum by M', and this set has a nonempty intersection with the Lagrange Spectrum. Specifically, the Lagrange Spectrum and the Markoff Spectrum are the same up until 3, that is, $L_{<3} = M'$. But this still doesn't explain how the two are related.

Let m be a Markoff number in the triple (x, y, m) with $x, y \leq m$. Then we have that m divides $x^2 + y^2$. To see this, consider the Markoff equation,

$$x^2 + y^2 + m^2 = 3mxy$$

$$x^2 + y^2 = (3xy - m)m$$

This in turn yields the congruence, $x^2 \equiv -y^2 \pmod{m}$. Since all the elements of a Markoff triple are relatively prime, the two congruences $xv \equiv \pm y \pmod{m}$ have the unique solutions u and u', where $u, u' > 0$ and $u, u' < m$. Furthermore the congruences,

$$x^2u^2 \equiv y^2 \equiv -x^2 \pmod{m}$$

$$x^2 \equiv -y^2 \pmod{m}$$

together imply that $u^2 \equiv -1 \pmod{m}$. The same holds true for u' as well. The number u is called the *characteristic number* for the Markoff triple (x, y, m). Since $u^2 \equiv -1 \pmod{m}$ there exists a $\nu > 0$ such that $u^2 = -1 + \nu m$. This brings us to the next definition.

DEFINITION 4. The Markoff form $f_m(x, y)$ associated with the Markoff triple (x_m, y_m, m) with $x_m, y_m \leq m$ and characteristic number u, with $u^2 = -1 + \nu m$, is given by,

$$f_m(x, y) = mx^2 + (3m - 2u)xy + (\nu - 3u)y^2$$

Since $u^2 = -1 + \nu m$ the discriminant of the form is,

$$\Delta = (3m - 2u)^2 - 4(m)(\nu - 3u)$$

$$= 9m^2 + 4(u^2 - \nu m)$$

$$= 9m^2 - 4$$

Also note that for the Markoff form f_m,

$$m(f_m) = \inf\{|f_m(x, y)| : f_m(x, y) \neq 0 \text{ with } x, y \in \mathbb{Z}\} = m$$

Finally, it can be seen that,

$$\begin{aligned} M(f_m) &= \frac{\sqrt{\Delta}}{m(f_m)} \\ &= \frac{\sqrt{9m^2-4}}{m} \end{aligned}$$

Markoff himself proved that every form f with $M(f) < 3$ is equivalent to a Markoff form and since he also showed that the two spectra are equal below 3, we can now see the connection between the Markoff numbers and the Lagrange Spectrum. Cusick and Flahive [**6**], provide an elegant proof as to why the arithmetic minimum $m(f_m)$ is equal to m. For a more complete and thorough explanation of the history of the Markoff equation and the Unicity conjecture, see Aigner [**1**].

In the definition of the Markoff form, the form f_m depended on the Markoff triple (x, y, m). However, there could possibly be more than one Markoff triple that has maximal element m. This observation leads to two interesting questions. The first, does every Markoff number exist as the maximum element of a Markoff triple, and secondly, can it appear as the maximum element in more than one Markoff triple? It turns out that the first question is quite easy to answer, but the second is exactly the Unicity conjecture.

We now look at a summary of Baragar's Results.

Definition 5. Let I be and integral domain. A function $N : I \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is said to be a *norm* on I.

The norm on an integral domain can be thought of as a way of measuring the "size" of one of its elements. Although the base definition of a norm requires the image of an element to be a positive integer, we can extend the idea of a norm to create a *field norm*. For a quadratic field $K = \mathbb{Q}(\sqrt{D})$, we define the field norm to be $N : K \to \mathbb{Q}$ by $N(x + \sqrt{D}y) = x^2 - Dy^2$.

THEOREM 11 (Baragar 1996). *If either $m, 3m-2$, or $3m+2$ is a prime, twice a prime, or four times a prime, then there exists at most one integer pair (x, y) so that (x, y, m) is a Markoff Triple.*

This theorem relies on fixing a Markoff number m and considering the remaining quadratic as a norm equation in a real quadratic field:

$$x^2 + y^2 - 3mxy = -m^2$$

Which can be written in the form:

$$\alpha^2 - D\beta^2 = -m^2$$

where $\alpha = \left(\frac{2y-3xz}{2}\right)$ and $\beta = \frac{x}{2}$ and $D = 9m^2 - 4 = (3m+2)(3m-2)$.

At this point, we can see where the $3m-2$ and $3m+2$ originate. This equation which resulted from fixing a Markoff number m, is the same as the norm for the quadratic field $\mathbb{Q}(\sqrt{D})$, and can be shortened to,

$$N_{K/\mathbb{Q}}(\gamma) = -m^2$$

where γ is an element of $R = \mathbb{Z} + \omega\mathbb{Z}$, the ring of integers of $K = \mathbb{Q}(\omega)$ where ω is the largest solution to the equation $x^2 + 3mx + 1 = 0$. By considering the Markoff equation as a norm equation, Baragar reformulates the uniqueness condition in his second theorem.

THEOREM 12 (Baragar). *If m is an odd Markoff number, then m is the maximal element of a unique Markoff triple if and only if there exists exactly one pair of principal ideals $\gamma R, \bar{\gamma} R$ in R such that γ satisfies the norm equation above.*

Baragar notes that since the norm of γR is relatively prime to the discriminant $\Delta = 9m^2 - 4$, the factorization of γR in R is unique. It is also important to note that since $\gcd(x, y, m) = 1$, the ideal γR is a *primitive ideal.* That is, γR cannot be written as nJ where J is an R-ideal and $n \in \mathbb{Z}$. This leads to the following corollary.

COROLLARY 13. *If m is an odd prime Markoff number, then m is the maximal element of a unique Markoff triple.*

PROOF. Assume that m is a prime Markoff number, then the ideal mR is either a prime ideal or splits into two prime ideals, ρ and $\bar{\rho}$ (i.e. $mR = \rho\bar{\rho}$). Since γR is a primitive ideal and $m \in \mathbb{Z}$, we have that $\gamma R \neq mR$. Therefore, $mR = \rho\bar{\rho}$, and γR is equal to either ρ^2 or $\bar{\rho}^2$. Since there is only a single pair, m is the maximal element of a unique Markoff triple, by the previous theorem. $\square$

Suppose, towards a contradiction, that both γ and δ are elements of R that satisfy the norm equation above which generate different pairs of ideals. Their corresponding R-ideals can be factored into prime ideals, which may have some factors in common, and the ones that aren't common must be conjugates. That is, $\gamma R = \rho_1\rho_2$ and $\delta R = \rho_1\bar{\rho}_2$, where ρ_1 and ρ_2 are not all of R. Consider the product of the two ideals, which yields,

$$\gamma\delta R = \rho_1^2\rho_2\bar{\rho}_2.$$

At this point it is important to mention equivalency of ideals. We say that two ideals I and J are *narrow class equivalent* if there exist $\alpha_1, \alpha_2 \in R$ with $N(\alpha_1)$, $N(\alpha_2) > 0$, such that $\alpha_1 I = \alpha_2 J$ and denote the equivalence by $I \overset{+}{\sim} J$. If the restriction on the norms of α_1 and α_2 is removed, we say the two ideals are *class equivalent*, denoted by $I \sim J$. Returning to the ideals above, we see that R and ρ_1^2 are narrow class equivalent. Similarly, $R \overset{+}{\sim} \rho_2^2$ by considering the product of γR and ρR. Of these two possibilities, one of the ideals satisfies the inequality,

$$N(\rho_i) < m < \tfrac{1}{2}\sqrt{\Delta},$$

and so the goal is to classify all primitive ideals I in K which have norm less than $\frac{1}{2}\sqrt{\Delta}$ and also that $I \overset{+}{\sim} \bar{I}$. Baragar uses the following results,

LEMMA 14 (Baragar). *If I is a primitive ideal, then there exists a basis over $\mathbb{Z}$ for I of the form $r+\omega, N(I)$, for some $r \in \mathbb{Z}$. Furthermore, r may be chosen such that,*

$$\sqrt{\Delta} - N(I) < r + \omega \leq \sqrt{\Delta}.$$

COROLLARY 15. *If J is a primitive ideal and $J = \bar{J}$, then $N(J)$ divides Δ.*

LEMMA 16 (Baragar). *Suppose that $I \overset{+}{\sim} \bar{I}$. then there exists an ideal J in R such that J is primitive ideal, $N(J)$ divides Δ, and $I \sim J$.*

LEMMA 17. *Suppose a primitive ideal I satisfies $N(I) < \frac{1}{2}\sqrt{\Delta}$. Then x_I has a periodic continued fraction expansion, where*

$$x_I = \frac{r+\omega}{N(I)}.$$

Using the previous results, all the ideals I can be found by considering the periodic part of the continued fraction expansion of x_J for all ideals J with $N(J)$ dividing Δ. Baragar notes that for a fixed value of m this approach works well, but is if little use for arbitrary m. At this point we can finally address the case where $3m-2$ or $3m+2$ is a prime. If either is prime, then we will have that $N(I)$ divides Δ and as such, the ideals ρ_i cannot exist, yielding the contradiction. However, we need the next two lemmas.

Lemma 18. *Suppose $N(J) = t$ and $tu = 3m - 2$ with $u \in \mathbb{Z}$. That is, suppose $N(J)$ divides $3m - 2$. Then $N(I) = t$ or u.*

Lemma 19. *Suppose $N(J) = t$ and $tu = 3m + 2$ with $u \in \mathbb{Z}$ and $m > 3$. Then $N(I) = t$ or u.*

It is important to note that in both of the previous lemmas, if $N(J) = 3m \pm 2$ then J is a principal ideal. Together, these two theorems are used to prove the following corollary.

Corollary 20 (Baragar). *Suppose $p = 3m - 2$ or $3m + 2$ is prime, and p divides $N(J)$. Then there exists a J' such that $J \sim J'$ and $N(J')$ divides Δ/p.*

Proof. Suppose that $p = 3m - 2$ or $3m + 2$ is prime, and $p \mid N(J)$. Then the ideal $\rho = \left(\frac{p+\sqrt{\Delta}}{2}\right)\mathbb{Z} \times p\mathbb{Z}$ has norm p. By the previous lemmas, ρ is principal. Since J and ρ are principal, we have that $J \sim \rho J$. However, $N(\rho J)$ will not divide Δ, since $p^2 \nmid \Delta$, which implies that ρJ is not primitive. Let J' be the ideal such that $nJ' \sim \rho J$, where n is the largest factor of ρJ in $\mathbb{Z}$. Since p divides n, we have that $J' \sim J$ and $N(J') \mid \frac{\Delta p}{p^2} = \frac{\Delta}{p}$. $\square$

Therefore, by the corollary if $3m \pm 2$ is prime, then $N(I) \mid \Delta$, yielding our contradiction. $J \overset{+}{\sim} J'$.

We need only consider the case where m is even. Since the elements of a Markoff triple are relatively prime, the remaining two elements, x and y, must be both odd. We again consider the equation,

$$x^2 + y^2 - 3mxy = -m^2.$$

Since every Markoff number is either 1 or 2 modulo 4, we can rewrite the equation with $m = 2k$, where k is odd.

$$(x - 3ky)^2 - (9k^2 - 1)y^2 = -4k^2$$

Note that since x, y, and k are all odd, $x - 3ky$ is even and $9k^2 - 1$ is congruent to 0 modulo 4. Then, by dividing both sides by 4 we get the following equation,

$$\alpha^2 - \beta^2 y^2 = -k^2$$

where $\alpha = \frac{x-3ky}{2}$ and $\beta^2 = \frac{9k^2-1}{4}$. Baragar continues from here as before this time with $\omega = -3k + \sqrt{9k^2 - 1}$. Noting that the discriminant $\Delta = 9k^2 - 1$ is relatively prime to k, there is unique factorization of the ideals dividing k^2R, where $R = \mathbb{Z} + \beta\mathbb{Z}$. Continuing along the same path as before, suppose that there are two ideals γR and δR, and consider all possible ideals I which satisfy,

$$N(I) < k < \tfrac{1}{2}\sqrt{\Delta}.$$

Then if, $N(J) = t$ and $tu = \frac{3k-1}{2}$, we have that $N(I) = t$ or u as before and when $N(J) = \frac{3k-1}{2}$, we have that $u = 1$ and J is principal. Similarly, if $N(J) = t$ with $tu = \frac{3k+1}{2}$, $t, u \geq 2$, $N(I)$ divides Δ, and if $N(J) = \frac{3k+1}{2}$ J again is principal. Therefore, when $3m \pm 2$ is four times a prime, $N(I)$ divides Δ yielding our contradiction.

CHAPTER 4

ELEMENTARY METHODS

This chapter will discuss elementary methods of proofs for some of the earlier results. Some basic results about Markoff numbers will be used throughout this section.

(1) If (x, y, m) is a Markoff triple, then $\gcd(x, y, m) = 1$.

(2) Every odd Markoff number is congruent to 1 modulo 4.

(3) Every even Markoff number is congruent to 2 modulo 4.

(4) If m is an even Markoff number, then $\frac{3m-2}{4}$ and $\frac{3m+2}{8}$ are both odd integers.

This elementary proof is due to Srinivasan[**7**], and is a proof of uniqueness when m is a prime power or twice a prime power.

Lemma 21. *Let (x_1, y_1, m) and (x_2, y_2, m) be two Markoff triples. Then*

$$(x_1x_2 - y_1y_2)(x_1y_2 - y_1x_2) = m^2(x_1y_1 - x_2y_2).$$

Theorem 22. *If m is a Markoff number that is an odd prime power or two times an odd prime power, then m is unique.*

Proof. Let (x_1, y_1, m) and (x_2, y_2, m) be two Markoff triples with $x_i \leq y_i \leq m$. Suppose that $x_1y_1 - x_2y_2 = 0$. By the lemma we have that $(x_1x_2 - y_1y_2)(x_1y_2 - y_1x_2) = 0$ and so we have two cases,

$$x_1x_2 = y_1y_2 \text{ or } x_1y_2 = y_1x_2.$$

Consider the case where $x_1y_2 = y_1x_2$. Since (x_1, y_1, m) and (x_2, y_2, m) are Markoff triples, $\gcd(x_1, y_1) = 1$ and $\gcd(x_2, y_2) = 1$, so all primes dividing x_1 must divide x_2 and all primes dividing x_2 must divide x_1, and the same is true of y_1 and y_2. Therefore, it must be that $x_1 = x_2$ and $y_1 = y_2$. In the case where $x_1x_2 = y_1y_2$, it must be that $x_1 = y_2$ and $x_2 = y_1$, by the same argument as the first case. In both cases we have that $x_1y_1 - x_2y_2 \neq 0$. Let $g > 2$ be an odd prime divisor of m and suppose that $x_1x_2 \equiv y_1y_2 \pmod{g}$ and $x_1y_2 \equiv x_2y_1 \pmod{g}$. Then

$$x_1^2x_2y_2 \equiv x_1^2x_2y_2 \pmod{g}$$

which implies that,

$$x_1^2 \equiv y_1^2 \pmod{g}$$

since $\gcd(x_i, y_i, m) = 1$. Note that g also divides $x_1^2 + y_1^2$, but this is impossible since $\gcd(b_1, m) = 1$. Thus, it must be that

$$\gcd(x_1x_2 - y_1y_2, x_1y_2 - y_1x_2, m') = 1$$

where $m' = m$ when m is odd and $\frac{m}{2}$ when m is even. Then $m = pq$ or $m = 2pq$, depending on whether m is odd or even, respectively. We have that

$$x_1x_2 - y_1y_2 \equiv 0 \pmod{p^2} \text{ and } x_1y_2 - y_1x_2 \equiv 0 \pmod{q^2}$$

If m is an odd prime power or twice an odd prime power then either p or q must be 1. Then $p(\text{or } q) = m$ or $\frac{m}{2}$ based on the parity of m.

In the case where m is odd, then $x_1x_2 - y_1y_2 \equiv 0 \pmod{m^2}$ which implies that $x_1x_2 = y_1y_2$. However, since elements of Markoff triples are relatively prime, this cannot happen.

If m is even, then $x_1x_2 - y_1y_2 \equiv 0 \pmod 4$. Thus,

$$x_1x_2 - y_1y_2 \equiv 0 \ (\mathrm{mod}\ \tfrac{m^2}{4})$$

and because $\frac{m^2}{4}$ is odd, we have that $x_1x_2 - y_1y_2 \equiv 0 \pmod{m^2}$, which again leads to the same contradiction. □

The next proof, which is also due to Srinivasan, shows that if the largest factor of $3m - 2$ or $3m - 2$ is a prime power, then m is unique.

THEOREM 23. *Let m be a Markoff number such that the greatest odd divisor of either $3m - 2$ or $3m + 2$ is a prime power. Then m is unique.*

PROOF. Again let (x_1, y_1, m) and (x_2, y_2, m) be two Markoff triples and let $X_i = \frac{x_i - y_i}{2}$ and $Y_i = \frac{x_i + y_i}{2}$. Then it follows that,

$$(2 - 3m)X_1^2 + (2 + 3m)Y_1^2 = -m^2$$

$$(2 - 3m)X_2^2 + (2 + 3m)Y_2^2 = -m^2$$

and by subtracting the two previous equations,

$$(3m - 2)(X_1^2 - X_2^2) = (3m + 2)(Y_1^2 - Y_2^2).$$

Now, suppose that m is odd and that $3m + 2$ is a prime power of the prime p. If $p \mid \gcd(2(X_1 + X_2), 2((X_1 - X_2)))$, then $p \mid X_1$ and $p \mid m$, which is a contradiction. Thus, if $3m + 2$ is a prime power of p, then either $3m + 2 \mid 2(X_1 + X_2)$ or $3m + 2 \mid 2(X_1 - X_2)$, but since $x_iy_i \le m$ and $x_i \le \sqrt{m}$,

$$3m + 2 \le 2(X_1 + X_2) \le 2(m - 1) + 2\sqrt{m}.$$

If m is even, it is not divisible by 4 and we also have that both $\frac{3m-2}{4}$ and $\frac{3m+2}{8}$ are odd integers (as mentioned at the beginning of this chapter). Therefore, it must be that $2X_i$ is even and the x_i, y_i are all odd. This implies that the X_i, Y_i's are integers with X_i all odd and Y_i all even, since $X_i - Y_i = y_i$.

Finally, the case where $\frac{3m-2}{4}$ and $\frac{3m+2}{8}$ are prime powers are handled in the following way. Suppose $\frac{3m-2}{4}$ is a prime power. Then,

$$\frac{3m-2}{4}\frac{X_1^2 - X_2^2}{3m+2} = \frac{Y_1^2 - Y_2^2}{4}$$

is a false statement if $x_i \leq y_i \leq m$, and therefore $|\frac{Y_1+Y_2}{2}| \leq \frac{m}{2}$ $\square$

BIBLIOGRAPHY

[1] Martin Aigner, *Markov's theorem and 100 years of the uniqueness conjecture*, Springer, Cham, 2013. A mathematical journey from irrational numbers to perfect matchings. MR3098784

[2] Arthur Baragar, *On the unicity conjecture for Markoff numbers*, Canad. Math. Bull. **39** (1996), no. 1, 3–9, DOI 10.4153/CMB-1996-001-x. MR1382484 (97d:11110)

[3] Enrico Bombieri, *Continued fractions and the Markoff tree*, Expo. Math. **25** (2007), no. 3, 187–213, DOI 10.1016/j.exmath.2006.10.002. MR2345177 (2008h:11072)

[4] J. O. Button, *Markoff numbers, principal ideals and continued fraction expansions*, J. Number Theory **87** (2001), no. 1, 77–95, DOI 10.1006/jnth.2000.2578. MR1816037 (2002a:11074)

[5] Feng-Juan Chen and Yong-Gao Chen, *On the Frobenius conjecture for Markoff numbers*, J. Number Theory **133** (2013), no. 7, 2363–2373, DOI 10.1016/j.jnt.2012.12.018. MR3035968

[6] Thomas W. Cusick and Mary E. Flahive, *The Markoff and Lagrange spectra*, Mathematical Surveys and Monographs, vol. 30, American Mathematical Society, Providence, RI, 1989. MR1010419 (90i:11069)

[7] Anitha Srinivasan, *Markoff numbers and ambiguous classes*, J. Théor. Nombres Bordeaux **21** (2009), no. 3, 755–768 (English, with English and French summaries). MR2605546 (2011e:11118)

CURRICULUM VITAE

Graduate College

University of Nevada, Las Vegas

Brandon Metz

Home Address:

1101 Adelman Dr

Las Vegas, Nevada 89123

Degrees:

Bachelor of Science, Honors Mathematics, 2009

Elizabethtown College, Elizabethtown, USA

Thesis Title: A Comparison of Results on the Unicity Conjecture of the Markoff Equation

Thesis Examination Committee: Chairperson, Arthur Baragar, Ph.D.

Committee Member, Ebrahim Salehi, Ph.D.

Committee Member, Peter Shiue, Ph.D.

Graduate Faculty Representative, Stephen Miller, Ph.D.