Finding a Solution to the Diophantine Representation of the Primes

Nachiketa Gupta

A THESIS

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial Fulfillment of the Requirements for the Degree of Master of Arts

2003

Supervisor of Thesis

Graduate Group Chairperson

ABSTRACT

Finding a Solution to the Diophantine Representation of the Primes

Nachiketa Gupta

Advisor: Jean Gallier

Martin Davis, Yuri Matijasevic, and Julia Robinson wrote a paper together in 1976 titled "Hilbert's Tenth Problem. Diophantine Equations: Positive Aspects of a Negative Solution." In this paper they outline some results related to Hilbert's Tenth Problem. I could not stop thinking about the first one.

This was the formulation of a Diophantine system of equations such that a solution to the system would exist if and only if one particular variable is a prime number. We will show that the set of primes forms a recursively enumerable set, which will provide the intuition as to why there should exist a Diophantine representation for the set of primes.

Hilbert's Tenth Problem states that it is impossible to find an algorithm which will decide whether any given Diophantine equation has a solution. We will go through the necessary steps required to find a solution to the Diophantine representation for the set of primes. During this process, we will also show how to solve the Pell equation using continued fractions. As an example for the method, we shall also go through the prime number two.

Contents

1 Introduction and Background Information **1**

1.1 Introduction 1

1.2 Diophantine Equations 3

1.3 Pell Equation 3

2 The Set of Primes are Diophantine Representable **5**

2.1 Introduction 5

2.2 Recursively Enumerable Sets 6

2.3 Recursively Enumerable Sets are Diophantine Representable 7

2.4 Diophantine Representation of the Set of Primes 8

2.5 Hilbert's Tenth Problem 9

3 Continued Fractions **12**

3.1 Introduction 12

3.2 Simple Continued Fractions 12

3.3 Infinite Simple Continued Fractions 15

3.4 Quadratic Irrational 15

4 Solving the Pell Equation **18**

4.1 Introduction 18

4.2 Method and Example 19

4.3 Special Pell Equation 21

5 Solving the Diophantine System Representing the Set of Primes **23**

5.1 Introduction 23

5.2 Method 24

6 Example: Prime Two **28**

6.1 Introduction 28

6.2 Satisfying Set 28

6.3 Proof of Minimal Solution for a and o 33

6.4 The Other Four Variables 35

A Acknowledgements **39**

B Bibliography **41**

Chapter 1

Introduction and Background Information

1.1 Introduction

Martin Davis, Yuri Matijasevic, and Julia Robinson wrote a paper together in the *Proceedings of Symposia in Pure Mathematics* Volume 28, 1976 titled "Hilbert's Tenth Problem. Diophantine Equations: Positive Aspects of a Negative Solution" [DMR76]. In this paper they outline some important results arising from Hilbert's Tenth Problem. They are all absolutely wonderful results. However, I could not stop thinking about the first result. It is almost counter-intuitive.

This was the formulation of a system of polynomial equations with integer coefficients over integer solutions (we will later define this as Diophantine) such that a

positive solution to the system would exist if and only if one particular parameter was a prime number, while the others are unknown. The system consisted of 14 constraint Diophantine equations over 26 natural numbers. However, these numbers grow very quickly because the system is based on a representation of the exponential function. It is derived from the Diophantine representation for solutions to the Pell equation, the Diophantine representation of solutions to the exponential function, and the Diophantine representation of solutions to the factorial function.

A number of papers have been written in this area. They go into varying detail and reference heavily different papers. One of these was a paper by James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens titled *Diophantine Representation of the Set of Primes* [JSWW76]. This paper contained a nicely written proof of necessity and sufficiency for the validity of the system. However, it does call on other papers also for much of the background.

Another important paper is "Hilbert's Tenth Problem" by Martin Davis [Dav73]. This paper contains the derivation for the Diophantine system representing solutions to the Pell equation and the Diophantine system representing the exponential function. It also contains the "twenty-four easy lemmas" used to prove the validity of these two systems.

This paper will focus on providing some background to the Diophantine representation of the set of primes and how to go about solving it. In the process, we will explain recursively enumerable sets in order to provide some intuition for Diophan-

tine representations of a set. We will also discuss Hilbert's Tenth Problem and its implications. Then we will provide continued fractions as a method to solving the Pell equation. This will lead us directly into how we should find solutions to the Diophantine representation of the Set of Primes. Finally, we will use the prime number two as an example and attempt to solve the system. Some background information follows.

1.2 Diophantine Equations

We will talk about Diophantine equations throughout this paper. A Diophantine equation is an equation which can be expressed by $f = g$, where f and g are both polynomials. The coefficients of the polynomials must be integers and the solutions are required to be non-negative integers.

1.3 Pell Equation

As it turns out a significant number of the equations we will discuss are Pell Equations. The Pell equation is a special Diophantine equation of the form

$$x^2 - dy^2 = N. \tag{1.1}$$

This can be thought of as a special case of a diophantine equation of the form

$$ax^2 \pm by^2 = c, \tag{1.2}$$

or even further a special case of the bivariate Diophantine equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{1.3}$$

We can see that the bivariate Diophantine equation begins to look like the Pell equation when $a = 1, b = 0, d = 0$, and $e = 0$.

Also, notice the obvious solution to the Pell Equation when $N = 1$

$$x = 1, y = 0. \tag{1.4}$$

There are a number of "efficient" ways to find solutions to the Pell Equation. We will later discuss one very nice way.

Chapter 2

The Set of Primes are Diophantine Representable

2.1 Introduction

In this chapter, we will discuss what a recursively enumerable set is. Then we will show that the set of primes is a set that is recursively enumerable. This will provide us with the intuition as to why the set of primes should be Diophantine Representable. We will then give the Diophantine representation for this set.

In addition, we will then explain what Hilbert's Tenth problem is and how it ties in to the rest of this chapter.

2.2 Recursively Enumerable Sets

We will first introduce the idea of a recursively enumerable set. Other terms such as computably enumerable, listable, partially-decidable, semidecidable, or Turing-recognizable are often used to describe this set also. We will give some equivalent definitions below for recursively enumerable which will give some intuition as to why these different names are used.

Definition 2.1. A set S is called recursively enumerable if

(i) There is a Turing machine that enumerates exactly the members of S. (Therefore the terms Turing-recognizable and computably enumerable are often used.)

(ii) There is a well-defined algorithm to make a list of exactly the members of S. (Therefore the term listable is often used.)

(iii) It represents the range of a recursive function. Equivalently, S is recursively enumerable if there exists a recursive function that can eventually generate any element in S. (Therefore the term recursively enumerable is often used.)

(iv) Given an input x, there exists an algorithm A such that A halts and outputs YES if and only if x belongs to the set S. If x does not belong to the set S, the algorithm either runs forever, or halts and outputs NO. (Therefore the terms partially-decidable and semidecidable are often used.)

All of these definitions are equivalent. Please see [MY78] for further details. For the remainder of this paper, we will only use the term recursively enumerable.

We can now state the set of all prime numbers is recursively enumerable. It is easy to see this by Definition 2.1 (iv). Given a number n, we can test if it is prime by attempting to divide by every number less than n. Similarly, the exponential function (a^x) and the factorial function also define sets which are recursively enumerable since we can test membership of any number by a given algorithm

In the next section, we will state that all of these sets are in fact Diophantine representable.

2.3 Recursively Enumerable Sets are Diophantine Representable

As an even simpler example than the last two, we can state that the set of even numbers forms a recursively enumerable set, since we can test if a number is even with a simple algorithm. More so, since the set of even numbers is precisely $\{x$ such that there exists $y \in \mathbb{Z}$ and $y = 2x\}$, the Diophantine system representing even numbers is given by the single equation $y = 2x$ (where $x, y \in \mathbb{Z}$).

The main positive aspect of the negative solution to Hilbert's Tenth Problem is that every Diophantine set is a recursively enumerable set and every recursively enumerable set is Diophantine representable. For more information on this, please see [Mat70] and [DMR76].

Therefore, we know that the set of primes must also be Diophantine representable.

The question remains how to represent them. This was shown by Martin Davis, Yuri Matijasevic, and Julia Robinson.

The derivation of the system is out of the scope of this paper. If the reader is interested in seeing it, please refer to [JSWW76]. It would also be helpful to look through [Dav73] as a bare minimum. In the next section, we will give the Diophantine system.

2.4 Diophantine Representation of the Set of Primes

The system has been expressed in slightly different forms in different papers. There have been minor changes in representation only. Here is the system given by [JSWW76] with a slight modification so that all variables belong to the set of non-negative integers. In this system there is a solution for all variables if and only if $k + 2$ is prime.

$$q = wz + h + j, \tag{2.1}$$

$$z = (gk + 2g + k + 1)(h + j) + h, \tag{2.2}$$

$$16(k + 1)^3(k + 2)(n + 1)^2 + 1 = f^2, \tag{2.3}$$

$$e = p + q + z + 2n, \tag{2.4}$$

$$e^3(e + 2)(a + 1)^2 + 1 = o^2, \tag{2.5}$$

$$x^2 = (a^2 - 1)y^2 + 1, \tag{2.6}$$

$$u^2 = 16(a^2 - 1)r^2y^4 + 1, \tag{2.7}$$

$$(x + cu)^2 = ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1, \tag{2.8}$$

$$m^2 = (a^2 - 1)l^2 + 1, \tag{2.9}$$

$$l = k + i(a - 1), \tag{2.10}$$

$$n + l + v = y, \tag{2.11}$$

$$m = p + l(a - n - 1) + b(2a(n + 1) - (n + 1)^2 - 1), \tag{2.12}$$

$$x = q + y(a - p - 1) + s(2a(p + 1) - (p + 1)^2 - 1), \tag{2.13}$$

$$pm = z + pl(1 - p) + t(2ap - p^2 - 1). \tag{2.14}$$

It should also be noted that any system of Diophantine equations with real coefficients can be expressed as a single Diophantine equation by moving everything to the left side of each equation so the right side equals zero. Then we can simply square each equation and add them. So all variables will be on the left side of the Diophantine equation and the right side will simply be zero still. Since the left side is a sum of squares, each individual expression being squared must equal zero or else the right side would not be zero. This will be an important idea for the next section.

2.5 Hilbert's Tenth Problem

In 1900, the last year of the nineteenth century, during the *Second International Congress of Mathematicians* in Paris, Hilbert introduced twenty-three unsolved problems. These were problems that he felt were among the most important from the

nineteenth century and which would continue into the upcoming twentieth century. Since then, these have been labelled "Hilbert's Twenty-Three Problems."

What follow is a translation into English of the tenth problem exactly as it was stated:

> 10. Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

Equivalently, this can be stated as: Is it possible to find an algorithm which will tell us whether or not a polynomial Diophantine equation with integer coefficients has integer solutions?

A negative proof to Hilbert's Tenth Problem was given by Matijasevic in [Mat70]. He proved that every recursively enumerable set is Diophantine representable. More so, there are undecidable recursively enumerable sets such as x such that M_x halts on input x where M_x denotes the Turing Machine whose code is x. This is the set of codes that halts on itself as input. The problem of determining whether a code will halt on itself is called the Halting Problem. (A definition for Turing Machine can be found in [MY78]).

Now we would like to discuss how to solve the particular Diophantine system representing the set of primes. However, we will need to provide the next two chapters

before we can do this.

Chapter 3

Continued Fractions

3.1 Introduction

This chapter will introduce continued fractions and some properties. We will rely heavily on the information in this chapter for the next chapter, where we will show how to solve the Pell equation, when $N = 1$ in (1.1).

3.2 Simple Continued Fractions

Definition 3.1. Let us define a continued fraction as the expression:

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots}}}, \tag{3.1}$$

where $q_1, q_2, \ldots$ are defined to be positive reals without loss of generality since q_0 may be negative.

Now, let's define a simple continued fraction.

Definition 3.2. If $q_0, q_1, q_2, \ldots \in \mathbb{Z}$, then the continued fraction is called a simple continued fraction.

We should introduce some quick notation for the continued fraction also.

Definition 3.3. Use the notation $< q_0, q_1, q_2, q_3, \ldots >$ to express the continued fraction in Definition 3.1.

The following proposition is very easy to see from Definition 3.1, but will prove to be very useful in proofs later.

Proposition 3.1. $< q_0, q_1, \ldots, q_n, q_{n+1} >=< q_0, q_1, \ldots, q_{n-1}, q_n + \frac{1}{q_{n+1}} >$.

We will now define convergents of the continued fraction, which we will use in a later lemma.

Definition 3.4. Define $r_n =< q_0, q_1, \ldots, q_n >$, for every $n > 0$. These are called the convergents of the continued fraction.

We will now define two sequences of great importance to the study of continued fractions, and then state and prove a lemma relating the convergents from Definition 3.4 to these sequences.

Definition 3.5. Define $h_{-2} = 0, h_{-1} = 1, k_{-2} = 1, k_{-1} = 0$. For every $i \geq 0$, define

$$h_i = h_{i-1}q_i + h_{i-2}, \tag{3.2}$$

$$k_i = k_{i-1}q_i + k_{i-2}. \tag{3.3}$$

Lemma 3.1. *For every* $n \geq 0, r_n = \frac{h_n}{k_n}$.

Proof. We will prove this by induction. The base case $n = 0$ can be checked quickly:

$$r_0 = \frac{h_0}{k_0} = \frac{h_{-1}q_0 + h_{-2}}{k_{-1}q_0 + k_{-2}} = \frac{q_0}{1} = q_0. \tag{3.4}$$

For the induction hypothesis, assume $r_n = \frac{h_n}{k_n}$. Define

$$h' = (q_n + \frac{1}{q_{n+1}})h_{n-1} + h_{n-2}, \tag{3.5}$$

$$k' = (q_n + \frac{1}{q_{n+1}})k_{n-1} + k_{n-2}. \tag{3.6}$$

By Proposition 3.1 and the induction hypothesis, $\frac{h'}{k'} =< q_0, q_1, \ldots, q_k, q_{n+1} >$. Now let's look at h_{n+1} and k_{n+1}

$$h_{n+1} = h_n q_{n+1} + h_{n-1} = (h_{n-1}q_n + h_{n-2})q_{n+1} + h_{n-1}, \tag{3.7}$$

$$k_{n+1} = k_n q_{n+1} + k_{n-1} = (k_{n-1}q_n + k_{n-2})q_{n+1} + k_{n-1}. \tag{3.8}$$

However, it is easy to see now that

$$h' = \frac{h_{n+1}}{q_{n+1}}, k' = \frac{k_{n+1}}{q_{n+1}}. \tag{3.9}$$

So,

$$r_{n+1} = \frac{h_{n+1}}{k_{n+1}} = \frac{h'}{k'} =< q_0, q_1, \ldots, q_k, q_{n+1} > . \tag{3.10}$$

□

The value of the simple continued fraction is given by $lim_{n\to\infty} r_n$. We will simply mention that this limit will always exist. A proof of this can be found in [NZ72]

3.3 Infinite Simple Continued Fractions

In order to find solutions to the Pell equation, we must learn about the infinite simple continued fraction. This is exactly what it sounds like.

Lemma 3.2. *An infinite simple continued fraction* $< q_0, q_1, q_2, q_3, \ldots >$ *is irrational.*

A proof for this lemma can be found in [NZ72]. We must also learn about periodicity in the infinite simple continued fraction. We will see why this is important in the first theorem of Section 3.4.

Definition 3.6. An infinite simple continued fraction $< q_0, q_1, q_2, q_3, \ldots >$ is called periodic if and only if there exists $m > 0$ such that $q_{m+n} = q_n$ for all sufficiently large n.

In other words, a periodic simple continued fraction will begin to repeat itself from a certain point on. We will define notation below.

Definition 3.7. Use the notation $< q_0, q_1, q_2, \ldots, q_i, \overline{p_0, p_1, p_2, \ldots, p_j} >$ to express a periodic simple continued fraction where the bar over $p_0, p_1, p_2, \ldots, p_j$ indicates that it repeats itself infinitely.

3.4 Quadratic Irrational

The simple continued fraction representation of the quadratic irrational (square root of a non-square natural number) is one of the keys to solving the Pell equation as we will see below. The following theorem is a very important result for this.

Theorem 3.1. If an infinite simple continued fraction is periodic, it is a quadratic irrational.

Proof. **Case 1:** Simple continued fraction is purely periodic.

$$\beta =< \overline{p_0, p_1, p_2, \ldots, p_j} > . \tag{3.11}$$

Then we can say that,

$$\beta =< \overline{p_0, p_1, p_2, \ldots, p_j}, \beta > . \tag{3.12}$$

From Lemma 3.1, we know that

$$\beta = \frac{h_j\beta + h_{j-1}}{k_j\beta + k_{j-1}} \tag{3.13}$$

By rearranging, we know that β is a root of a quadratic equation. Since the simple continued fraction representation of β is infinite, by Lemma 3.2, we know that β must be a quadratic irrational.

Case2: Simple continued fraction is not purely periodic.

$$\alpha =< q_0, q_1, \ldots, q_i, \overline{p_0, p_1, p_2, \ldots, p_j} > . \tag{3.14}$$

Let us define β (similar to (3.11)) as

$$\beta =< \overline{p_0, p_1, p_2, \ldots, p_j} > . \tag{3.15}$$

Now we can write (similar to (3.12))

$$\alpha =< q_0, q_1, \ldots, q_i, \beta > . \tag{3.16}$$

We know that (similar to (3.13))

$$\alpha = \frac{h_i\beta + h_{i-1}}{k_i\beta + k_{i-1}} \tag{3.17}$$

We also know that β is of the form

$$\frac{a + \sqrt{b}}{c} \tag{3.18}$$

for some a, b, c. Again, by Lemma 3.2, we know that α cannot be rational. Then by (3.17) and (3.18), we know that α must be a quadratic irrational also. □

The converse of the above theorem also holds. A proof of this can be found in [NZ72].

Let's go through a quick example to make sure we understand this clearly before moving on to the next chapter.

Example 3.1. *Let us find x, where $x =< a, b, a, b, \ldots >=< \overline{a, b} >$. Alternatively, we can write x as*

$$x = a + \frac{1}{b + \frac{1}{x}}. \tag{3.19}$$

This is simply a quadratic, which we can solve. The solutions to this quadratic are

$$\frac{ab \pm \sqrt{a^2b^2 + 4ab}}{2b}. \tag{3.20}$$

Chapter 4

Solving the Pell Equation

4.1 Introduction

From here on, when we say Pell equation, we will always be talking about the special case of the Pell equation (1.1), when $N = 1$. In this chapter, we will walk through one way of solving the Pell equation. The basic idea will be to use the simple continued fraction representation of $\sqrt{d}$ (from (1.1)) to find the minimal solution of the Pell equation.

This chapter will provide many of the ideas necessary to solve the Diophantine system representing the set of primes in the next chapter.

4.2 Method and Example

The following lemma will provide some insight to Theorem 4.1 which will be used in solving the Pell equation.

Lemma 4.1. $h_i k_{i-1} - h_{i-1} k_i = (-1)^{i+1}$, *for every* $i \geq -1$

Proof. We will prove this by induction. The base case $i = -1$ can be checked quickly

$$h_{-1} k_{-2} - h_{-2} k_{-1} = 1 = (-1)^0. \tag{4.1}$$

For the induction hypothesis, assume $i = j \geq -1$. Then,

$$\begin{aligned} h_{j+1} k_j - h_j k_{j+1} &= (h_j q_{j+1} + k_{j-1}) k_j - h_j (k_j q_{j+1} + k_{j-1}) \\ &= -(h_j k_{j-1} - h_{j-1} k_j) \\ &= (-1)^{j+2}. \end{aligned} \tag{4.2}$$

□

Theorem 4.1. Calling m the length of the period of the radical $\sqrt{d}$,

$$h_{im-1}^2 - d k_{im-1}^2 = (-1)^{im}, \text{ for every } i \geq 0. \tag{4.3}$$

The proof for the above theorem is omitted, but can be found in [NZ72]. This shows how to solve the Pell Equation.

Noting that any solution to the Pell equation can be found by (4.3), we can find the nontrivial minimal solution to the Pell equation by choosing i that minimizes $im - 1 \geq 1$. Also, note that im must be even since we would like the right hand side of (4.3) to be 1. We should start an example here.

Example 4.1. *Let's look at the Pell equation* $x^2 - 7y^2 = 1$. *In this case,* $d = 7$. *The simple continued fraction representation of the radical* $\sqrt{d}$ *is* $< 2, \overline{1, 1, 1, 4} >$. *The period* m *equals* 4, *here. For the minimal solution, we pick* $i = 1$ *since* m *is even. (It should be obvious also that if* m *is odd, we pick* $i = 2$ *for the minimal solution). So,* $im - 1 = 3$ *and our minimal solution is* $(h_3, k_3) = (8, 3)$.

It should be noted that we can find all solutions to the Pell equation by exhausting all possibilities of i in the above Corollary (4.1), but the following lemma will provide an easier way of finding all other solutions.

Lemma 4.2. *Let* x_1, y_1 *be the minimal positive solution of Pell equation* $x^2 - dy^2 = 1$, *where* d *is positive and is not a perfect square. Then* x, y *is a non-negative solution if and only if* $x = x_n, y = y_n$ *for some* n, *where* $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.

A proof for this lemma can be found in [NZ72]. What follows is a very simple lemma to help us think more clearly.

Lemma 4.3. $x_{m\pm n} = x_m x_n \pm d y_m y_n$ *and* $y_{m\pm n} = x_n y_m \pm x_m y_n$.

Proof.

$$x_{m+n} + y_{m+n}\sqrt{d} = (x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d}) \tag{4.4}$$

$$= (x_m x_n + d y_m y_n) + (x_n y_m + x_m y_n)\sqrt{d}. \tag{4.5}$$

Similarly,

$$(x_{m-n} + y_{m-n}\sqrt{d})(x_n + y_n\sqrt{d}) = x_m + y_m\sqrt{d}, \tag{4.6}$$

implies

$$x_{m-n} + y_{m-n}\sqrt{d} = (x_m + y_m\sqrt{d})(x_n - y_n\sqrt{d}) \tag{4.7}$$

$$= (x_m x_n - d y_m y_n) + (x_n y_m - x_m y_n)\sqrt{d} \tag{4.8}$$

Note that we used the fact that $x_n^2 - d y_n^2 = 1$ above since x_n and y_n are solutions to our Pell equation. □

4.3 Special Pell Equation

In this section, we will look at the special case of the Pell equation (1.1) where

$$d = a^2 - 1, a > 1, N = 1. \tag{4.9}$$

Notice that in this case, we have another obvious solution, in addition to (1.4):

$$x_1 = a, y_1 = 1. \tag{4.10}$$

Below, we will give a simple Corollary from Lemma 4.2.

Corollary 4.1. Let us define $x_n = x_n(a)$ and $y_n = y_n(a)$ such that all solutions to this special Pell equation must be of this form:

$$x_n + y_n\sqrt{d} = (a + \sqrt{d})^n, \text{ for every } a > 1 \text{ and for every } n \geq 0. \tag{4.11}$$

This corollary is very easy to see by a simple substitution from (4.10).

The following Corollary is a special case of Lemma 4.3, when $n = 1$ for the special Pell equation.

Corollary 4.2. $x_{m\pm1} = ax_m \pm dy_m$ and $y_{m\pm1} = ay_m \pm x_m$.

Proof. Letting $n = 1$ in Lemma (4.3), we have

$$x_{m\pm1} = x_m x_1 \pm dy_m y_1, \tag{4.12}$$

$$y_{m\pm1} = x_1 y_m \pm x_m y_1. \tag{4.13}$$

Remembering that $x_1 = a$ and $y_1 = 1$, let's make these substitutions into (4.12) so we get $x_{m\pm1} = ax_m \pm dy_m$ and $y_{m\pm1} = ay_m \pm x_m$. □

Chapter 5

Solving the Diophantine System Representing the Set of Primes

5.1 Introduction

The proof of the system given in Section 2.4 is provided with an excellent explanation in [JSWW76]. There are also other papers with the proof provided. So, I will not repeat it here. Instead, I will provide some insight into how to solve the system, given the proof.

As I go through the method for solving the system, I will drop some ideas from the proof to help explain what we are doing. It will quickly become obvious that this Diophantine representations for the set of primes relies heavily on the Pell equation, exponential function, and factorial function. However, I strongly recommend reading

the proof for a complete understanding.

Also, I should again mention here that we are solving the representation provided earlier in Section 2.4. The original representation by Matiyasevich in 1970 differed somewhat ([Mat70]). There were also a number of other Diophantine representations of the primes with less variables. However, with less variables, the polynomial degree of the Diophantine system increased greatly. A description of these along with some other Diophantine representations are provided in [Rib91].

5.2 Method

For the system to be satisfied, we assume a selected value of $k \geq 0$ and $k+2$ is a prime number. Let's provide Wilson's Theorem as our first lemma here.

Lemma 5.1 (Wilson's Theorem). *For every, $k \geq 0, k+2$ is a prime number if and only if $(k+2)|((k+1)!+1)$.*

A proof of this lemma can be found in [NZ72]. This lemma tells us that if $k+2$ is prime, we can pick a number g such that

$$(k+1)! = gk + 2g + k + 1. \tag{5.1}$$

Note that this means $(k+1)!+1 = (g+1)(k+2)$. Let us now give the following lemma which defines the factorial function by a Diophantine system.

Lemma 5.2. *In order for $f_k = k+1!$ for $f_k, k \geq 0$, it is necessary and sufficient that*

there exists $f, h, j, n, p, q, w,$ *and* $z \geq 0$ *such that*

$$q = wz + h + j, \tag{5.2}$$

$$z = f_k(h + j) + h, \tag{5.3}$$

$$16(k+1)^3(k+2)(n+1)^2 + 1 = f^2, \tag{5.4}$$

$$p = (n+1)^{k+1}, \tag{5.5}$$

$$q = (p+1)^n, \tag{5.6}$$

$$z = p^{k+2}. \tag{5.7}$$

A proof for this lemma can be found in [JSWW76]. Now, we can choose f and n that satisfy (5.4) (or equivalently (2.3)) (note that this is a Pell Equation and we can find all solutions by using Corollary 4.1 of which we can pick the minimal solution if desired). Next, we use (5.5),(5.6), and (5.7) to find values for p, q, and z quickly. We will use the following three equations to find solutions for h, j, and w. It is very easy to see that the three of these come directly from (5.2) and (5.3). (Note that q mod z simply means the remainder left after dividing q by z).

$$w = \lfloor \frac{q}{z} \rfloor, \tag{5.8}$$

$$h = z - (k+1)! \cdot (q \bmod z), \tag{5.9}$$

$$j = (q \bmod z) - h. \tag{5.10}$$

Then, we can choose e that satisfies (2.4) easily. We can choose $a \geq 2$ and o that satisfy (2.5) by noticing that this is also a Pell equation. Let

$$y = y_n(a) \tag{5.11}$$

(from Definition 4.1). Next, let us give the following lemma which defines a particular solution to the Pell equation.

Lemma 5.3. *In order for $y = y_n(a)$ for $a \geq 2$ and $n \geq 1$, it is necessary and sufficient that there exists c, d, r, u, and x such that*

$$x^2 = (a^2 - 1)y^2 + 1, \tag{5.12}$$

$$u^2 = 16(a^2 - 1)r^2y^4 + 1, \tag{5.13}$$

$$(x + cu)^2 = ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1, \tag{5.14}$$

$$n \leq y. \tag{5.15}$$

A proof for this lemma can also be found in [JSWW76]. The first three equations above are exactly the same as (2.6), (2.7), and (2.8). We can find x satisfying the Pell equation (2.6). Then, we can find u and r again by solving the Pell equation (2.7).

Finally, we can find c and d satisfying the Pell equation (2.8). We know that a solution exists since a, x, y, and u are now fixed. So the remaining equation in (2.8) is simply a Pell equation on variables c and d.

$$m = x_{k+1}(a) \tag{5.16}$$

and

$$l = y_{k+1}(a). \tag{5.17}$$

This will satisfy (2.9). Choose i, v, b, s, and t that satisfy (2.10), (2.11), (2.12),(2.13), and (2.14), respectively. If any of these do not turn out to be integers, we will have to make another choice for the solution of the Pell equation we chose earlier.

Again, we did not completely show necessity and sufficiency above. Instead we can find this is in [JSWW76]. In the next section, we will go through the example of the prime 2, where we try to solve for all variables.

Chapter 6

Example: Prime Two

6.1 Introduction

In this chapter, we will attempt to find a solution of the Diophantine representation of the set of primes for the prime 2 using the techniques discussed throughout this paper.

6.2 Satisfying Set

(1) Choose $k = 0$ for prime 2.

(2) After substituting k into (5.1) we have

$$(0+1)! = g \cdot 0 + 2g + 0 + 1, \tag{6.1}$$

$$1 = 2g + 1. \tag{6.2}$$

Choose $g = 0$ to satisfy this equation.

(3) After substituting k into (2.3) we have

$$16(0+1)^3(0+2)(n+1)^2+1 = f^2, \tag{6.3}$$

$$f^2 - 32(n+1)^2 = 1 \tag{6.4}$$

In order to find f and n, we must find a solution to the Pell equation (6.4). The continued fraction representation of $\sqrt{32} =< 5, \overline{1,1,1,10} >$. So, if we choose the minimal solution, we have $(f, n+1) = (h_3, k_3)$. This gives $(f, n) = (17, 2)$.

(4) After substituting k and n into (5.5) we have

$$p = (2+1)^{0+1} \tag{6.5}$$

Choose $p = 3$ to satisfy this equation.

(5) After substituting n and p into (5.6) we have

$$q = (3+1)^2 \tag{6.6}$$

Choose $q = 16$ to satisfy this equation.

(6) After substituting k and p into (5.7) we have

$$z = 3^{0+2} \tag{6.7}$$

Choose $z = 9$ to satisfy this equation.

(7) After substituting q and z into (5.8) we have

$$w = \lfloor \frac{16}{7} \rfloor \tag{6.8}$$

Choose $w = 1$ to satisfy this equation.

(8) After substituting k, q, and z into (5.9) we have

$$h = 9 - (0+1)! \cdot (16 \bmod 9), \tag{6.9}$$

$$h = 9 - (7). \tag{6.10}$$

Choose $h = 2$ to satisfy this equation.

(9) After substituting h, q, and z into (5.10) we have

$$j = (16 \bmod 9) - 2, \tag{6.11}$$

$$j = (7) - 2. \tag{6.12}$$

Choose $j = 5$ to satisfy this equation.

(10) After substituting n, p, q, and z into (2.4) we have

$$e = 3 + 16 + 9 + 2(2) \tag{6.13}$$

Choose $e = 32$ to satisfy this equation.

(11) After substituting e into (2.5) we have

$$32^3(32+2)(a+1)^2 + 1 = o^2, \tag{6.14}$$

$$o^2 - 2^{16}17(a+1)^2 = 1 \tag{6.15}$$

In order to find a, o, we must find a solution to the Pell equation (6.15). The minimal solution given our selection of variables thus far gives

$$a = 790169035809889616168555687974994918632638071340929091 2 \text{ and}$$

$$o = 834035301564579468329946270481226888212608613465610836377 7.$$

To see why, please see the next section.

(12) After substituting n into (5.11) we have

$$y = y_2(a) \tag{6.16}$$

We know that the minimal solution $(x_1, y_1) = (a, 1)$ from (4.10). So $y_2 = 2a$ by Corollary 4.2 here.

(13) We can now either solve (5.12) directly or we can note that since $y = y_2(a)$, x must be $x_2(a)$ in order to be a solution pair to the Pell equation. $x_2(a) = ax_1 + (a^2 - 1) = 2a^2 - 1$. We used (4.10) and Corollary 4.2 here.

(14) After substituting k into (5.16) and (5.17) we have

$$m = x_{0+1}(a) = a \tag{6.17}$$

$$l = y_{0+1}(a) = 1 \tag{6.18}$$

We used (4.10) here.

(15) After substituting k, l into (2.10) we have

$$1 = 1 + i(a - 1) \tag{6.19}$$

Since we know $a-1 \neq 0$, we choose $i=0$ to satisfy this equation.

(16) After substituting l, n, y into (2.11) we have

$$2+1+v=2a \tag{6.20}$$

We choose $v=2a-3$ to satisfy this equation.

(17) After substituting l, m, n, p into (2.12) we have

$$\begin{aligned} a &= 3+1(a-2-1)+b(2a(2+1)-(2+1)^2-1), && (6.21)\\ a &= 3+a-3+b(6a-9-1), && (6.22)\\ 0 &= b(6a-10). && (6.23)\\ & && (6.24) \end{aligned}$$

Since we know $6a-10 \neq 0$, choose $b=0$ to satisfy this equation.

(18) After substituting p, q, x, y into (2.13) we have

$$\begin{aligned} 2a^2-1 &= 16+2a(a-3-1)+s(2a(3+1)-(3+1)^2-1), && (6.25)\\ 2a^2-1 &= 16+2a^2-8a+s(8a-16-1), && (6.26)\\ 8a-17 &= s(8a-17). && (6.27)\\ & && (6.28) \end{aligned}$$

Since we know $8a-17 \neq 0$, choose $s=1$ to satisfy this equation.

(19) After substituting l, m, p, z into (2.14) we have

$$\begin{aligned} 3 \cdot a &= 9 + 3 \cdot 1(a-3) + t(2a \cdot 3 - 3^2 - 1), && (6.29) \\ 3a &= 9 + 3a - 9 + t(6a - 10), && (6.30) \\ 0 &= t(6a - 10). && (6.31) \\ & && (6.32) \end{aligned}$$

Since we know $6a - 10 \neq 0$, choose $t = 0$ to satisfy this equation.

We provided values for 22 of the 26 variables above (for the prime 2). There will be a note about the other four in section 6.4. It should also be noted that we attempted to pick the smallest values for each variable whenever possible given past choices. This does not ensure that each variable above has the smallest possible value for the prime two. However, for many of the large variables it is unlikely that there will be smaller possible values.

6.3 Proof of Minimal Solution for a and o

We would like to find the minimal solution of the Pell equation $o^2 - 2^{16}17(a+1)^2 = 1$ or equivalently, $x^2 - 2^{16}17y^2 = 1$, where $x = o$ and $y = a + 1$.

Let's look at two ways of doing this. The first way will be the same method we have been using thus far, while the second way will investigate a slightly different way.

Method 1

The continued fraction representation of $\sqrt{2^{16} \cdot 17} =< 1055, \overline{1, 1, 16, 8, 5, 2, 1, 1, 2, 1, 2,}$ $\overline{32, 1, 1, 1, 1, 1, 1, 2, 3, 2, 7, 1, 4, 3, 1, 1, 2, 1, 131, 4, 1, 1, 4, 3, 7, 1, 14, 1, 1, 8, 32, 1, 6, 1, 1, 5, 2,}$ $\overline{1, 7, 1, 1, 3, 1, 1, 1, 2, 527, 2, 1, 1, 1, 3, 1, 1, 7, 1, 2, 5, 1, 1, 6, 1, 32, 8, 1, 1, 14, 1, 7, 3, 4, 1, 1, 4,}$ $\overline{131, 1, 2, 1, 1, 3, 4, 1, 7, 2, 3, 2, 1, 1, 1, 1, 1, 1, 32, 2, 1, 2, 1, 1, 2, 5, 8, 16, 1, 1, 2110} >$. This has period 116. So, we want $(x, y) = (h_{115}, k_{115})$. This gives $(x, y) = (834035301564579$ $468329946270481226888212608613465610836377 7, 790169035809889616168555687974$ $994918632638071340929091 3)$. This is the smallest possibility for x, y since we picked the minimal solution here.

However, in this method, we did not discuss how we generated the continuous fraction and how we knew the period is 116. Let us look at another approach below, which may be much easier to do in some cases.

Method 2

Let's look at the similar Pell equation where d is square free: $X^2 - 17Y^2 = 1$. The continued fraction representation of $\sqrt{17} =< 4, \overline{8} >$. So, we want $(X, Y) = (h_1, k_1)$. This gives $(X, Y) = (33, 8)$. We now want to find the minimal solution of this same Pell equation restricting the second term to be divisible by $\sqrt{2^{16}} = 2^8$. In this way, we can find a solution to the original Pell equation.

First we note that in this case, X_n is always odd. The following lemma will prove this.

Lemma 6.1. *X_n satisfying $X^2 - 17Y^2 = 1$ is odd for every $n \geq 1$.*

Proof. This will be a proof by induction. The base case holds since $X_1 = 33$. Assume for our induction hypothesis that X_n is odd for $n = m$. We will now want to show that it is also odd for X_{m+1}. $X_{m+1} = 33X_m + 17 \cdot 8Y_m$ (use Lemma 4.3). From our induction hypothesis, the first term is odd. It is obvious that the second term is even. Therefore, X_{m+1} is odd. □

Next, we notice that $Y_{2n} = 2X_nY_n$. It is easy to see that we need to choose Y_{2^5} to make sure that it is divisible by 2^8 (this can be proven by Lemma 4.3). Now we notice that when we go back to the original Pell equation, we can choose $o = X_{2^5}$ and $a+1 = \frac{Y_{2^5}}{2^8}$. By Lemma 4.2, this gives $a = 790169035809889616168555687974994918632638071$ 3409290912 and $o = 834035301564579468329946270481226888212608613465610836377 7$ like before.

6.4 The Other Four Variables

We can certainly show how to find the variables c, d, r, u, which are missing above. However, these variables grow to be so large that it would be physically impossible to compute them.

Let's apply the process used in Method 2 above to (2.7). Let's look at the similar Pell equation where d is square free: $U^2 - (a^2 - 1)R^2 = 1$. In this case we will want to find the minimal solution of this Pell equation with the restriction that R is divisible

by $\sqrt{16y^4} = 4y^2$. This would give us a solution to our original Pell equation. The prime factorization of $4y^2$ is

$$2^{16}691^2357348514747598415416314981898966587659478143696151^2.$$

This means that we would need at least $y_{3573485147475984154163149818989665876594781436961 51}$ (by Lemma 6.3) which is already more than 10^{52} decimal places (we will show why later).

We can see that u must be even bigger than r by the Pell equation. The numbers c and d are part of another Pell equation in (2.8) that rely on a value of u (and are probably even larger than u).

Lemma 6.2.

$$(x_n, y_n) = 1.$$

Proof. Assume $k|x_n, k|y_n$, then $k|(x_n^2 - dy_n^2)$. This implies $k|1$ since $x_n^2 - dy_n^2 = 1$. □

Lemma 6.3. *Let p be a prime and let n be the smallest positive integer such that p divides y_n. Assume in addition that p^2 does not divide y_n. Then y_{np} is the smallest value that is divisible by p^2.*

Proof. Assume p^2 divides y_m for some $m < np$. Then $m = kn + r$, where $0 \leq r < n$

and $k > 0$. Then, we have

$$\begin{aligned} x_r + y_r\sqrt{d} &= (x_1 + y_1\sqrt{d})^r && (6.33)\\ &= (x_1 + y_1\sqrt{d})^{m-kn} && (6.34)\\ &= (x_1 + y_1\sqrt{d})^m \cdot (x_1 + y_1\sqrt{d})^{-kn} && (6.35)\\ &= (x_1 + y_1\sqrt{d})^m \cdot (x_1 - y_1\sqrt{d})^{kn} && (6.36)\\ &= (x_m + y_m\sqrt{d}) \cdot (x_n - y_n\sqrt{d})^k && (6.37) \end{aligned}$$

Since both y_m and y_n are divisible by p we conclude that y_r is also divisible by p. But n was chosen as the smallest positive integer, such that p divides y_n. Therefore, r must be 0 and n divides m so that $m = kn$ for some $k > 1$.

So we have

$$\begin{aligned} x_{kn} + y_{kn}\sqrt{d} &= (x_n + y_n\sqrt{d})^k && (6.38)\\ &= \sum_{i=0}^{k} \binom{k}{i} x_n^{k-i} (y_n\sqrt{d})^i. && (6.39) \end{aligned}$$

This implies

$$y_m = y_{kn} = \sum_{i \ odd, 1 \le i \le k} \binom{k}{i} x_n^{k-i} y_n^i d^{\frac{i-1}{2}} \qquad (6.40)$$

If $i \geq 2$, then p^2 obviously divides y_n^i since p divides y_n. But we also need the term for $i = 1$ to be divisible by p^2. This term is

$$k x_n^k y_n. \qquad (6.41)$$

Since x_n and y_n are relatively prime (by Lemma 6.2), we also know that x_n and p are relatively prime since p divides y_n. Further, since p^2 does not divide y_n, we must

have p divides k. So, we pick $k = p$. This is a contradiction of our assumption that $m < np$ since $m = kp = np$. Further, we see that y_{np} is the smallest solution divisible by p^2. (Note that x_i and y_i are obviously both increasing functions with respect to i.)

□

Last but not least, lets mention how we arrive at 10^{52} decimal places? We know

$$y_i = \frac{1}{2\sqrt{d}}((x_i + \sqrt{d}y_i) - (x_i - \sqrt{d}y_i)) \tag{6.42}$$

$$= \frac{1}{2\sqrt{d}}((x_1 + \sqrt{d}y_1)^i - (x_1 + \sqrt{d}y_1)^{-i}) \tag{6.43}$$

The second term in the above equation decreases exponentially, so we ignore it for large i. So, y_i must be very close to

$$\frac{1}{2\sqrt{d}}(x_1 + \sqrt{d}y_1)^i \tag{6.44}$$

If we take the logarithm base 10, we can approximate the number of decimal places for y_i to be

$$i \cdot log(x_1 + \sqrt{d}y_1). \tag{6.45}$$

Appendix A

Acknowledgements

Special thanks to (in alphabetical order):

Dr. Martin Davis for some e-mail correspondence.

Dr. Dennis DeTurck for acting on my academic committee and discussing the details of the paper with me.

Dr. Herbert Enderton for some discussion meetings.

Dr. Jean Gallier for acting as my academic advisor for this research. He also introduced me to [DMR76], which began my interest in this whole area.

Dr. Yuri Matiyasevich for some e-mail correspondence and introducing me to Dr. Vsemirnov.

Dr. Max Mintz for acting as my academic advisor in the Computer Science Department and providing me with academic guidance.

Dr. Maxim Vsemirnov for kindly providing much assistance and guidance via only

e-mail correspondence and proofreading the entire thesis.

And last but not least, the Mathematics Faculty and Staff at the University of Pennsylvania for providing me with the facilities and guidance to complete this research. The Mathematics Department not only contains a unique faculty and student body but also a wonderful staff.

On another note, I should also thank the researchers of Hilbert's Tenth Problem. There are so many people who made significant contributions here.

Bibliography

[Buc46] R. C. Buck. Prime-representing functions. *American Mathematical Monthly*, 53(5):265, May 1946.

[Dav73] Martin Davis. Hilbert's Tenth Problem is unsolvable. *The American Mathematical Monthly*, 80(3):233–269, March 1973. Reprinted with corrections in the Dover edition of Davis [1958].

[Dav82] Martin Davis. *Computability and Unsolvability*. Dover, 1982.

[DMR76] Martin Davis, Yuri Matijasevič, and Julia Robinson. Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution. In *Mathematical Developments Arising from Hilbert Problems*, volume 28 of *Proceedings of Symposia in Pure Mathematics*, pages 323–378, Providence, Rhode Island, 1976. American Mathematical Society.

[Dud69] Underwood Dudley. History of a formula for primes. *American Mathematical Monthly*, 76(1):23–28, January 1969.

[HW79] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford Clarendon Press, fifth edition, 1979.

[Jon82] James P. Jones. Universal Diophantine equation. *Journal of Symbolic Logic*, 47(3):549–571, September 1982.

[JSWW76] James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens. Diophantine representation of the set of prime numbers. *The American Mathematical Monthly*, 83(6):449–464, June–July 1976.

[Len02] Lenstra. Solving the pell equation. *NOTICES: Notices of the American Mathematical Society*, 49, 2002.

[Mat70] Ju. V. Matijasevič. Enumerable sets are Diophantine. *Soviet Mathematics. Doklady*, 11(2):354–358, 1970.

[Mat93] Yu. V. Matiyasevich. *Hilbert's Tenth Problem.* MIT Press, Cambridge, Massachusetts, 1993.

[Mat00] Matiyasevich. Hilbert's tenth problem: What was done and what is to be done. In Denef, Lipshitz, Pheidas, and Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, AMS, 2000.* 2000.

[MY78] Michael Machtey and Paul Young. *An Introduction to the General Theory of Algorithms.* Thomond Books, 1978.

[NZ72] I. Niven and H. S. Zuckerman. *An Introduction to the Theory of Numbers*. Wiley, 1972.

[Rei43] Irving Reiner. Functions not formulas for primes. *American Mathematical Monthly*, 50(10):619–621, December 1943.

[Rib91] Paulo Ribenboim. *The Little Book of Big Primes*. Springer-Verlag, New York, 1991.

[Sma98] Nigel P. Smart. *The Algorithmic Resolution of Diophantine Equations*. Cambridge University Press, 1998.

[Sør97] Morten Heine Sørensen. Hilbert's tenth problem. In *Computability and Complexity from a Programming Perspective (D-295)*, Foundations of Computing, pages 167–185. MIT Press, Boston, London, 1 edition, 1997.

[ST86] T. N. Shorey and R. Tidjeman. *Exponential Diophantine Equations*. Cambridge University Press, 1986.

[Wri51] E. M. Wright. A prime-representing function. *American Mathematical Monthly*, 58(9):616–618, November 1951.