Hilbert's Tenth Problem

Nicole Bowen

B.S., Mathematics

An Undergraduate Honors Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Bachelor of Science

at the

University of Connecticut

May 2014

May 2014

APPROVAL PAGE

Bachelor of Science Honors Thesis

Hilbert's Tenth Problem

Presented by

Nicole Bowen, B.S. Math

Honors Major Advisor _____
William Abikoff

Honors Thesis Advisor _____
David Reed Solomon

University of Connecticut

May 2014

ACKNOWLEDGMENTS

Many thanks to Professor Solomon for helping me through all the details of Hilbert's Tenth Problem, and for undertstanding that things always take longer than expected.

Hilbert's Tenth Problem

Nicole Bowen, B.S.

University of Connecticut, May 2014

ABSTRACT

In 1900, David Hilbert posed 23 questions to the mathematics community, with focuses in geometry, algebra, number theory, and more. In his tenth problem, Hilbert focused on Diophantine equations, asking for a general process to determine whether or not a Diophantine equation with integer coefficients has integer solutions. Seventy years later, Yuri Matiyasevich and his colleagues showed that such a process does not exist, with a proof that has had many applications for modern computability theory. In this thesis, we give a background on Diophantine equations and computability theory, followed by an in-depth explanation of the unsolvability of Hilbert's Tenth Problem.

Contents

Part I

Introduction

In countless areas of mathematics, finding solutions to equations is a necessity. Often, such solutions are sought over the real numbers. However, in some cases, one may attempt to find solutions that are more restricted, perhaps to certain subsets of the reals. For example, say we are dealing with an equation whose x and y variables represent the number of horses and sheep on a farm. In this example, a solution of say $x = \sqrt{2}$ and $y = -16$ is not so meaningful, so we may want to restrict our solutions to the natural numbers.

Such examples were the focus for a Greek mathematician named Diophantus (200's A.D.), who was concerned with finding only natural or positive rational number solutions to equations, as he considered other values to be nonsensical. Thus, equations whose solutions are restricted to the natural numbers, integers, or rationals are often called Diophantine equations.

Even today, many Diophantine equations remain difficult to solve. In particular, the methods for finding solutions vary depending on the number of variables and the degree of an equation. As either of these increase, it becomes more and more difficult to solve the equation, to the point where we still do not have complete methods to do so. One particular difficulty when attempting to solve Diophantine equations is that we may not be sure that a solution even exists, and thus any attempt to find one may be in vain.

In 1900, David Hilbert asked for a method to help solve this dilemma in what came to be known as Hilbert's tenth problem. In particular, the problem was given as follows:

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.

In 1970, a Russian mathematician named Yuri Matiyasevich found that such a process does not exist, with the help of his colleagues Martin Davis, Julia Robinson, and Hilary Putnam. His proof, which has had many applications in modern computability theory, is described in detail in this thesis.

Part II

Background: Diophantine Equations and Sets

Chapter 1

Key Definitions and Concepts

1.1 Diophantine Equations

In order to understand Hilbert's tenth problem, we must first know what a Diophantine equation is. In general, a Diophantine equation is classified not only by its form, but also by the range of its unknowns, which are often restricted to the rationals, integers, or natural numbers. For our purposes, we will define a Diophantine equation based on the specifications that Hilbert used in the statement of his problem. When Hilbert states "rational integers", he was refering to the integers, so we can define a Diophantine equation as follows:

Definition 1.1.1. A *Diophantine equation* is an equation of the form

$$D(x_1, ..., x_m) = 0$$

where D is a polynomial with integer coefficients, and where solutions for $x_1, ..., x_m$ are restricted to the integers.

1.2 Simplifying Hilbert's Problem

As previously stated, when Hilbert posed his tenth problem, he wanted a method for determining whether or not *integer* solutions exist for any Diophantine equation.

In this section, we will see that it is equivalent to work in the natural numbers, which for our purposes will include 0. It is important to note that for a particular Diophantine equation, the problem of deciding whether or not it has integer solutions is a different problem from deciding whether or not it has natural number solutions. However, in terms of deciding whether or not a general process exists for checking the solvability of an equation, it is equivalent to work with the natural numbers. In other words, we will see in this section that there is a general process for determining whether or not Diophantine equations have natural number solutions if and only if there is a general process for determining whether or not Diophantine equations have integer solutions.

First, we will show that if there is no general process for checking the existance of natural number solutions, there there is no general process for checking the existance of integer solutions. Note that we can take a system of Diophantine equations and compress it into a single Diophantine equation. In particular, the system

$$\begin{gathered} D_1(x_1, ..., x_m) = 0 \\ \vdots \\ D_k(x_1, ..., x_m) = 0 \end{gathered}$$

has an integer solution $x_1, ..., x_m$ if and only if the Diophantine equation

$$D_1^2(x_1, ..., x_m) + ... + D_k^2(x_1, ..., x_m) = 0$$

has an integer solution $x_1, ..., x_m$.

Now, let $D(x_1, ..., x_m) = 0$ be any arbitrary Diophantine equation, and let $E(x_1, ..., x_m, y_{1,1}, ..., y_{m,4}) = 0$ be the Diophantine equation formed by compressing the system

$$\begin{gathered} D(x_1, ...,x_m) = 0 \\ x_1 = y_{1,1}^2 + y_{1,2}^2 + y_{1,3}^2 + y_{1,4}^2 \\ \vdots \\ x_m = y_{m,1}^2 + y_{m,2}^2 + y_{m,3}^2 + y_{m,4}^2. \end{gathered}$$

If $D(x_1, ..., x_m) = 0$ has a solution in the natural numbers, then $E(x_1, ..., x_m, y_{1,1}, ..., y_{m,4}) = 0$ must have a solution in the integers, since any natural number can be written as the sum of four squares. Likewise, if $E(x_1, ..., x_m, y_{1,1}, ..., y_{m,4}) = 0$ has a solution in the integers, then $D(x_1, ..., x_m) = 0$ must have a solution in the natural numbers. Thus, any arbitrary Diophantine equation $D(x_1, ..., x_m) = 0$ has natural number solutions if and only if $E(x_1, ..., x_m, y_{1,1}, ..., y_{m,4}) = 0$ has an integer solu-

tion. So, if we were to find that there is no method of checking whether or not $D(x_1, ..., x_m) = 0$ has natural number solutions, then there is no way of checking whether or not $E(x_1, ..., x_m, y_{1,1}, ..., y_{m,4}) = 0$ has integer solutions. This means that we cannot check the existance of integer solutions for any arbitrary Diophantine equation,as E is one such equation.

Next, we will show that if there is a general process for checking natural number solutions, then there is a general process for checking integer solutions. Suppose that an arbitrary Diophantine equatio $D(x_1, ..., x_m) = 0$ has a solution in the integers. Note that any integer x_k can be written as the difference of two natural numbers a_k and b_k. Thus, the Diophantine equation $D(a_1 - b_1, ..., a_m - b_m) = 0$ must have a solution for $a_1, ..., a_m, b_1, ..., b_m$ in the natural numbers. Likewise, if $D(a_1 - b_1, ..., a_m - b_m) = 0$ has a solution for $a_1, ..., a_m, b_1, ..., b_m$ in the natural numbers, then $x_1 = a_1 - b_1, ..., x_m = a_m - b_m$ is a solution to $D(x_1, ..., x_m) = 0$ in the integers. Thus, any arbitrary Diophantine equation $D(x_1, ..., x_m) = 0$ is solvable in the integers if and only if the Diophantine equation $D(a_1 - b_1, ..., a_m - b_m) = 0$ is solvable in the natural numbers. So, if we were to find that there is a method of checking whether or not any Diophantine equation if solvable in the natural numbers, then we would know that there is a method of finding whether or not $D(a_1 - b_1, ..., a_m - b_m) = 0$ is solvable in the natural numbers. And if we can check the existance of solutions for $D(a_1 - b_1, ..., a_m - b_m) = 0$ in the natural numbers, then we can check the existance of integer solutions for any arbitrary $D(x_1, ..., x_m) = 0$.

With this, the question of the solvability of Hilbert's problem in the integers is reducible to the question of its solvability in the natural numbers. In general, this will make our work in proving that Hilbert's tenth problem is unsolvable easier, as it allows us to work within the natural numbers only. For the remainder of this thesis, all lowercase variables can be assumed to be natural numbers, unless otherwise stated.

1.3 Diophantine Sets

With the definition of a Diophantine equation in hand, we can define another important object of study, called a Diophantine set.

Definition 1.3.1. Let S be a set of n-tuples of natural numbers. Then S is called a *Diophantine set* if there exists some Diophantine equation $D(a_1, ..., a_n, x_1, ..., x_m)$, with parameters $a_1, ..., a_n$ and unknowns $x_1, ..., x_m$, such that

$$\langle a_1, ..., a_n \rangle \in S \iff \exists x_1, ..., x_m [D(a_1, ..., a_n, x_1, ..., x_m) = 0].$$

In order to understand this definition, it is perhaps best to look at some examples.

Example 1.3.2. Let $S = \{3\}$, and consider the equation

$$D(a, x) = (x + 1)(a - 3).$$

First, suppose $a \in S$. Then $a = 3$, so $D(a, x) = (x + 1)(a - 3) = 0$ for all x. Instead, suppose $a \notin S$. Then $a \neq 3$, so $a-3 \neq 0$. Then, since $x \in \mathbb{N}$, $D(a, x) = (x+1)(a-3) \neq 0$ for all x. Therefore, we can conclude that S is a Diophantine set, since we have found a Diophantine equation $D(a, x)$ such that $a \in S \iff \exists x[D(a, x) = 0]$.

Example 1.3.3. Let $S = \{3, 5\}$. Then consider the Diophantine equation

$$D(a, x) = (x + 1)(a - 3)(a - 5).$$

By the same reasoning described in the previous example, $a \in S \iff \exists x[D(a, x) = 0]$. Therefore, S is a Diophantine set.

1.4 Diophantine Functions, Relations, and Properties

In the previous section, we found that the sets $S = \{3\}$ and $S = \{3, 5\}$ were Diophantine. In some cases, rather than showing that a set of particular n-tuples is Diophantine, we may want to show that a set of n-tuples with certain properties is Diophantine, as in the next example.

Example 1.4.1. Let $S = \{\langle a, b, c\rangle | a + b = c\}$, and let

$$D(a, b, c, x) = (x + 1)(a + b - c).$$

Then $\langle a, b, c\rangle \in S \iff \exists x[D(a, b, c, x) = 0]$, so S is a Diophantine set.

In this example, rather than concluding that the set $S = \{\langle a, b, c\rangle | a + b = c\}$ is a Diophantine set, we might instead state that addition is a Diophantine function.

Definition 1.4.2. A function of natural numbers is a *Diophantine function* when its set of solutions is a Diophantine set.

In the next example, we show that multiplication is a Diophantine function.

Example 1.4.3. Let $S = \{\langle a, b, c\rangle | ab = c\}$, and let

$$D(a, b, c, x) = (x + 1)(ab - c).$$

Then $\langle a, b, c\rangle \in S \iff \exists x[D(a, b, c, x) = 0]$, so S is a Diophantine set.

Similarly, we can show that many relations are Diophantine.

Definition 1.4.4. A relation between n natural numbers is a *Diophantine relation* when the set of all n-tuples for which the relation holds is a Diophantine set.

In the following example, we show that the *less than* (and likewise *greater than*) relation is Diophantine.

Example 1.4.5. Let $S = \{\langle a, b\rangle | a < b\}$, and let

$$D(a, b, x) = (b - a) - (x + 1).$$

Then $\exists x[D(a, b, x) = (b - a) - (x + 1) = 0] \iff \exists x[b - a = x + 1] \iff a < b$. Therefore, S is a Diophantine set.

Similarly, the relation *less than or equal to* (and likewise *greater than or equal to*) is Diophantine.

Example 1.4.6. Let $S = \{\langle a, b\rangle | a \leq b\}$. Then consider the equation

$$D(a, b, x) = (b - a) - x.$$

Then $\exists x[D(a, b, x) = (b - a) - x = 0] \iff \exists x[b - a = x] \iff a \leq b$. Therefore, S is a Diophantine set.

The relation of divisibility is also Diophantine.

Example 1.4.7. Let $S = \{\langle a, b\rangle \mid a|b\}$, and let

$$D(a, b, x) = ax - b.$$

Then $\exists x[D(a, b, x) = ax - b = 0] \iff \exists x[ax = b] \iff a|b$. Therefore, S is a Diophantine set.

Further, we can show that certain properties are Diophantine.

Definition 1.4.8. A property of natural numbers is a *Diophantine property* when the set of numbers for which this property holds is Diophantine.

In the following example, we see that the property *is an even number* is Diophantine.

Example 1.4.9. . Let S be the set of all even numbers, and let

$$D(a, x) = 2x - a.$$

Then $a \in S \iff \exists x[D(a, x) = 0]$, so S is a Diophantine set.

We will also note that for any Diophantine function, relation, or property $X(a_1, ..., a_n)$, the condition

$$\exists x_{k+1}, ..., x_n[X(a_1, ..., a_k, x_{k+1}, ..., x_n)]$$

is also Diophantine. In other words, if the set

$$\{\langle a_1, ..., a_n\rangle \mid X(a_1, ..., a_n)\}$$

is a Diophantine set, then the set

$$\{\langle a_1, ..., a_k\rangle \mid \exists x_{k+1}, ..., x_n[X(a_1, ..., a_k, x_{k+1}, ..., x_n)]\}$$

is also a Diophantine set. For example, suppose there is some Diophantine relation R. Then there must exist a Diophantine equation $D(a_1, ..., a_n, x_1, ..., x_m)$ such that

$$R(a_1, ..., a_n) \iff \exists x_1, ..., x_m[D(a_1, ..., a_n, x_1, ..., x_m) = 0].$$

Then it follows that

$$\exists x_1, ..., x_{m+k}[D(a_1, ..., a_{n-k}, x_1, ..., x_{m+k}) = 0] \iff \exists x_1, ..., x_k[R(a_1, ..., a_{n-k}, x_1, ..., x_k)].$$

Thus the set

$$\{\langle a_1, ..., a_{n-k}\rangle \mid \exists x_1, ..., x_k[R(a_1, ..., a_{n-k}, x_1, ..., x_k)]\}$$

is a Diophantine set as well.

1.5 Unions and Intersections of Diophantine Sets

In this section, we will see that the union and intersection of Diophantine sets is also Diophantine.

Proposition 1.5.1. *The union of two Diophantine sets of n-tuples is Diophantine.*

Proof. Suppose that S_1 and S_2 are two Diophantine sets of n-tuples. Then there must be Diophantine equations D_1 and D_2 such that

$$\langle a_1, ..., a_n\rangle \in S_1 \iff \exists x_1, ..., x_m[D_1(a_1, ..., a_n, x_1, ..., x_m) = 0]$$

and

$$\langle a_1, ..., a_n\rangle \in S_2 \iff \exists y_1, ..., y_l[D_2(a_1, ..., a_n, y_1, ..., y_l) = 0].$$

Then consider the equation

$$D_3(a_1, ..., a_n, x_1, ..., x_m, y_1, ..., y_l) = D_1(a_1, ..., a_n, x_1, ..., x_m) \cdot D_2(a_1, ..., a_n, y_1, ..., y_l).$$

Then

$$\exists x_1, ..., x_m, y_1, ..., y_l[D_3(a_1, ..., a_n, x_1, ..., x_m, y_1, ..., y_l) = 0]$$

$$\iff \exists x_1, ...,x_m[D_1(a_1, ..., a_n, x_1, ..., x_m) = 0] \text{ or } \exists y_1, ..., y_m[D_2(a_1, ..., a_n, y_1, ..., y_l) = 0]$$

$$\iff \langle a_1, ..., a_n\rangle \in S_1 \text{ or } \langle a_1, ..., a_n\rangle \in S_2$$

$$\iff \langle a_1, ..., a_n\rangle \in S_1 \cup S_2.$$

Therefore, $S_1 \cup S_2$ is a Diophantine set.

□

Further note that this proposition can be interpreted in terms of Diophantine functions, relations, and properties using the conjunction "or".

Proposition 1.5.2. *The intersection of two Diophantine sets of n-tuples is Diophantine.*

Proof. Suppose that S_1 and S_2 are two Diophantine sets of n-tuples. Then there must be Diophantine equations D_1 and D_2 such that

$$\langle a_1, ..., a_n\rangle \in S_1 \iff \exists x_1, ..., x_m[D_1(a_1, ..., a_n, x_1, ..., x_m) = 0]$$

and

$$\langle a_1, ..., a_n\rangle \in S_2 \iff \exists y_1, ..., y_l[D_2(a_1, ..., a_n, y_1, ..., y_l) = 0].$$

Then consider the equation

$$D_3(a_1, ..., a_n, x_1, ..., x_m, y_1, ..., y_l) = D_1^2(a_1, ..., a_n, x_1, ..., x_m) + D_2^2(a_1, ..., a_n, y_1, ..., y_l).$$

Then

$$\exists x_1, ..., x_m, y_1, ..., y_l[D_3(a_1, ..., a_n, x_1, ..., x_m, y_1, ..., y_l) = 0]$$

$$\iff \exists x_1, ...,x_m[D_1(a_1, ..., a_n, x_1, ..., x_m) = 0] \text{ and } \exists y_1, ..., y_m[D_2(a_1, ..., a_n, y_1, ..., y_l) = 0]$$

$$\iff \langle a_1, ..., a_n\rangle \in S_1 \text{ and } \langle a_1, ..., a_n\rangle \in S_2$$

$$\iff \langle a_1, ..., a_n\rangle \in S_1 \cap S_2.$$

Therefore, $S_1 \cap S_2$ is a Diophantine set. □

Further note that this proposition can be interpreted in terms of Diophantine functions, relations, and properties using the conjunction "and".

Up until now, in order to show that a set is Diophantine, we have had to find a particular Diophantine equation that fits Defintion 1.3.1. However, with the results of this section, we can show that a set is Diophantine by representing it as the union or intersection of other Diophantine sets, as shown in the following example.

Example 1.5.3. Consider the function $rem(b, c)$, the remainder on dividing b by c. Then notice that

$$a = rem(b, c) \iff a < c \text{ and } c \mid (b - a)\,.$$

We have seen that the sets $S_1 = \{\langle a, b, c\rangle \mid a < c\}$ and $S_2 = \{\langle a, b, c\rangle \mid c|(b - a)\}$ are Diophantine sets. Then since $S = \{\langle a, b, c\rangle \mid a = rem(b, c)\} = S_1 \cap S_2$, S is Diophantine.

We will also mention that while the intersection and union of Diophantine sets remains Diophantine, the complement of a Diophantine set may not be Diophantine. In fact, we will see that the unsolvability of Hilbert's Tenth Problem results in part from the fact that there are Diophantine sets whose complements are not Diophantine. For examples of such sets, see [1, pgs 57-66].

Chapter 2

More Examples

We have now examined a number of Diophantine sets. Throughout our proof of Hilbert's tenth problem, we will use the fact that these and many other sets are Diophantine. Thus, we devote this chapter to a study of more examples that will be useful later.

2.1 More Diophantine Relations

The relation *equal to* is Diophantine.

Example 2.1.1. Let $S = \{\langle a, b\rangle \mid a = b\}$, and let

$$D(a, b, x) = (x + 1)(a - b).$$

Then $\exists x[D(a, b, x) = (x + 1)(a - b) = 0] \iff a = b \iff \langle a, b\rangle \in S$, so S is a Diophantine set.

Likewise, the relation *not equal to* is Diophantine.

Example 2.1.2. Let $S = \{\langle a, b\rangle \mid a \neq b\}$, and let

$$D(a, b, x) = (x + 1) + (a - b)^2.$$

Then $\exists x[D(a, b, x) = (x+1)+(a-b)^2 = 0] \iff \exists x[(a-b)^2 = x+1] \iff \langle a, b\rangle \in S$, so S is a Diophantine set.

Also, the relation *does not divide* is Diophantine.

Example 2.1.3. Let $S = \{\langle a, b\rangle \mid a \not| b\}$. Note that

$$a \not| b \iff rem(b, a) > 0.$$

We have already seen that the set $S_1 = \{\langle a, b, c\rangle \mid c = rem(b, a)\}$ is a Diophantine set. Further, we see that the set $S_2 = \{\langle a, b, c\rangle \mid c > 0\}$ is Diophantine by considering the equation $D(a, b, c, x) = (c - (x + 1))(a + 1)(b + 1)$, as

$$\begin{aligned} \exists x[D(a, b, c, x) = (c - (x + 1))(a + 1)(b + 1) = 0] &\iff \exists x[c - (x + 1) = 0] \\ &\iff \exists x[c = x + 1] \\ &\iff c > 0. \end{aligned}$$

Then $S = S_1 \cap S_2$, where S_1 and S_2 are Diophantine sets, so S is a Diophantine set.

The congruence relation is also Diophantine.

Example 2.1.4. Let $S = \{\langle a, b, c\rangle \mid a \equiv b(\mathrm{mod} c)\}$. Note that

$$a \equiv b(\mathrm{mod} c) \iff rem(a, c) = rem(b, c).$$

Then since we have seen that the *rem* function and *equal to* relation are Diophantine, we know that S is Diophantine as well.

2.2 More Diophantine Functions

Define the function $arem(b, c)$ to be the least absolute value $|X|$ among all numbers X congruent to b mod c. In other words,

$$arem(b, c) \equiv \pm b \bmod c \ \&\ 0 \leq arem(b, c) \leq \frac{c}{2}.$$

For example, while $rem(8, 5) = 3$, $arem(8, 5) = 2$. The function $arem(b, c)$ is Diophantine.

Example 2.2.1. Let $S = \{\langle a, b, c\rangle \mid a = arem(b, c)\}$. Note that

$$a = arem(b, c) \iff 2a \leq c \ \&\ [c \mid (b - a) \text{ or } c \mid (b + a)].$$

Since we have seen that the *less than or equal to* and *divides* relations are Diophantine, we know that S is Diophantine as well.

The choose function is also Diophantine.

Example 2.2.2. Let $S = \{\langle a, b, c\rangle \mid \binom{a}{b} = c\}$. For a proof that this set is Diophantine, see [1,pgs 44-45].

The function $b\ div\ c$, defined to be the integer part of $\frac{b}{c}$, is also Diophantine.

Example 2.2.3. Let $S = \{\langle a, b, c\rangle \mid a = b\ div\ c\}$. Note that

$$a = b\ div\ c \iff ac + rem(b, c) = b.$$

Then since we have seen that multiplication, addition, and the rem function are Diophantine, we know that S is Diophantine as well.

2.3 Another Diophantine Function:Exponentiation

In contrast to the examples that we have seen so far, it is actually quite difficult and technical to prove that exponentiation is a Diophantine function, i.e that the set $\{< a, b, c > |a = b^c\}$ is a Diophantine set. At first glance, we might attempt to prove such a fact by using an equation such as $D(a, b, c, x) = (x + 1)(b^c - a)$. The problem, however, is that this equation is not a polynomial, because of the term b^c, and therefore is not Diophantine. Thus, we will instead attempt to find a set of Diophantine conditions on a, b, and c that hold if and only if $a = b^c$. As it turns out, this is hard to do and requires a number of different steps. In fact, the proof that exponentiation is Diophantine is perhaps one of the most difficult steps in proving the unsolvability of Hilbert's Tenth Problem. We will now turn our attention to this proof.

2.3.1 Overview of the Proof

In order to prove that exponentiation is Diophantine, we must prove that the set

$$\{\langle a, b, c\rangle | a = b^c\}$$

is a Diophantine set. We note that the powers of any given b can be expressed as a recurrent sequence β_b, where

$$\beta_b(0) = 1 \quad \text{and} \quad \beta_b(n + 1) = b\beta_b(n).$$

Thus, another way to show that exponentiation is Diophantine would be to show that the set

$$\{< a, b, c > | a = \beta_b(c)\}$$

is a Diophantine set. However, it turns out that it is actually easier to work with another recurrent sequence α_b, where $b \geq 2$ and

$$\alpha_b(0) = 0 \quad \alpha_b(1) = 1 \quad \text{and} \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n).$$

First, we will examine some important properties of α_b. Then, we will prove that the sets

$$S = \{< a, b > | b \geq 2 \ \& \ \exists n[a = \alpha_b(n)]\}$$

and

$$S_* = \{< a, b, c > | b \geq 4 \ \& \ a = \alpha_b(c)\}$$

are Diophantine sets. Lastly, we will attempt to express β_b in terms of α_b in order to show that exponentiation is in fact Diophantine.

2.3.2 Examining the Sequence α_b

First, we will give a formal definition of α_b.

Definition 2.3.1. Let the second-order recurrent sequence α_b be defined for $b \geq 2$ as

$$\alpha_b(0) = 0 \quad \alpha_b(1) = 1 \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n).$$

While this is the definition of α_b we will use most often, in some cases it will be easier to use the equivalent form given in Proposition 2.3.2.

Proposition 2.3.2. *It is equivalent to define α_b with*

$$\alpha_b(n-2) = b\alpha_b(n-1) - \alpha_b(n).$$

Proof. From our initial definition of α_b we have that $\alpha_b(n) = b\alpha_b(n-1) - \alpha_b(n-2)$. Rearranging the terms in this equality yields $\alpha_b(n-2) = b\alpha_b(n-1) - \alpha_b(n)$. □

With these definitions of α_b in hand, we can start to investigate some of its properties. One especially important property of α_b is its increasing nature.

Proposition 2.3.3. *The sequence α_b is strictly increasing, i.e.*

$$0 = \alpha_b(0) < \alpha_b(1) < ... < \alpha_b(n) < \alpha_b(n+1) < ...$$

Proof. For the base case, let $n = 1$.
Since $\alpha_b(1) = 1$ and $\alpha_b(0)$=0, we have that

$$\alpha_b(0) \ < \ \alpha_b(1).$$

Then for the induction case, assume for all $n \leq k$ that

$$\alpha_b(n-1) \ < \ \alpha_b(n).$$

We need to show that $\alpha_b(k) < \alpha_b(k+1)$.
By our definition of α_b, we know that

$$\alpha_b(k+1) = b\alpha_b(k) - \alpha_b(k-1),$$

and by our induction hypothesis, we know that

$$\alpha_b(k-1) \ < \ \alpha_b(k).$$

Therefore, we get that

$$\alpha_b(k+1) = b\alpha_b(k) - \alpha_b(k-1) \ > \ b\alpha_b(k) - \alpha_b(k) \ = \ (b-1)\alpha_b(k) \ \geq \ \alpha_b(k).$$

Thus, by induction, for all $n \geq 1$,

$$\alpha_b(n-1) \ < \ \alpha_b(n).$$

□

The increasing nature of α_b can be seen in the following example.

Example 2.3.4. For b=2, the first ten terms of α_b are

$$\begin{aligned}
&\alpha_2(0) = 0\\
&\alpha_2(1) = 1\\
&\alpha_2(2) = 2\alpha_2(1) - \alpha_2(0) = 2(1) - 0 = 2\\
&\alpha_2(3) = 2\alpha_2(2) - \alpha_2(1) = 2(2) - 1 = 3\\
&\alpha_2(4) = 2\alpha_2(3) - \alpha_2(2) = 2(3) - 2 = 4\\
&\alpha_2(5) = 2\alpha_2(4) - \alpha_2(3) = 2(4) - 3 = 5\\
&\alpha_2(6) = 6\\
&\alpha_2(7) = 7\\
&\alpha_2(8) = 8\\
&\alpha_2(9) = 9
\end{aligned}$$

This example also demonstrates a convenient pattern of α_b that occurs when $b = 2$.

Proposition 2.3.5. *When $b = 2$, $\alpha_b(n) = n$ for all n.*

Proof. For the base case, let $n = 0$. Then $\alpha_2(0) = 0$. Let $n = 1$. Then $\alpha_2(1) = 1$. For the induction case, assume that $\alpha_2(n) = n$ for all $n \leq k$. We need to show that $\alpha_2(k+1) = k+1$. By our induction hypothesis, $\alpha_2(k+1) = 2\alpha_2(k) - \alpha_2(k-1) = 2k - (k-1) = k+1$. Thus, by induction, $\alpha_2(n) = n$ for all n. □

Unfortunately, Proposition 2.3.5 does not necessarily hold for larger values of b, as shown by the following example.

Example 2.3.6. For $b = 3$, the first ten terms of α_3 are

$$\begin{aligned}
&\alpha_3(0) = 0\\
&\alpha_3(1) = 1\\
&\alpha_3(2) = 3\alpha_3(1) - \alpha_3(0) = 3(1) - 0 = 3\\
&\alpha_3(3) = 3\alpha_3(2) - \alpha_3(1) = 3(3) - 1 = 8\\
&\alpha_3(4) = 3\alpha_3(3) - \alpha_3(2) = 3(8) - 3 = 21\\
&\alpha_3(5) = 3\alpha_3(4) - \alpha_3(3) = 3(21) - 8 = 55\\
&\alpha_3(6) = 144\\
&\alpha_3(7) = 377\\
&\alpha_3(8) = 987\\
&\alpha_3(9) = 2584
\end{aligned}$$

However, there is a weaker form of Proposition 2.3.5 that holds for general b.

Proposition 2.3.7. *For all n, $\alpha_b(n) \geq n$.*

Proof. We have seen that this proposition is true for $b = 2$, so assume that $b \geq 3$. Our proof will proceed by induction. For base cases, we have $\alpha_b(0) = 0$ and $\alpha_b(1) = 1$. For the induction case, assume that for all $n \leq k$, $k \neq 0$, that $n \leq \alpha_b(n)$. We need to show that $k + 1 \leq \alpha_b(k + 1)$. We find that

$$\begin{aligned}
\alpha_b(k+1) &= b\alpha_b(k) - \alpha_b(k-1) \text{ by definition} \\
&\geq b\alpha_b(k) - \alpha_b(k) \text{ since } \alpha_b \text{ is increasing by Proposition2.3.3} \\
&= (b-1)\alpha_b(k) \\
&\geq (b-1)k \text{ by our induction hypothesis} \\
&\geq 2k \text{ since we assumed } b \geq 3 \\
&\geq k+1 \text{ since } k \neq 0.
\end{aligned}$$

Therefore, by induction, $\alpha_b(n) \geq n$ for all n. □

We can also compare the values of α_b for different values of b.

Proposition 2.3.8. *If $b_1 \equiv b_2 \bmod q$, then $\alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \bmod q$ for all n.*

Proof. For the base case, let $b_1 \equiv b_2 \bmod q$. Then $\alpha_{b_1}(0) = 0$ and $\alpha_{b_2}(0) = 0$, so $\alpha_{b_1}(0) \equiv \alpha_{b_2}(0) \bmod q$. Also, $\alpha_{b_1}(1) = 1$ and $\alpha_{b_2}(1) = 1$, so $\alpha_{b_1}(1) \equiv \alpha_{b_2}(1) \bmod q$. Further, $\alpha_{b_1}(2) = b_1\alpha_{b_1}(1) - \alpha_{b_1}(0) = b_1 - 0 = b_1$ and $\alpha_{b_2}(2) = b_2\alpha_{b_2}(1) - \alpha_{b_2}(0) = b_2$, so by our assumption $\alpha_{b_1}(2) \equiv \alpha_{b_2}(2) \bmod q$.

For the induction case, assume that $\alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \bmod q$ for all $n \leq k$. We need to show that $\alpha_{b_1}(k+1) \equiv \alpha_{b_2}(k+1) \bmod q$.
By definition,

$$\begin{aligned}
\alpha_{b_1}(k+1) &= b_1\alpha_{b_1}(k) - \alpha_{b_1}(k-1) \\
\alpha_{b_2}(k+1) &= b_2\alpha_{b_2}(k) - \alpha_{b_1}(k-1).
\end{aligned}$$

So

$$\begin{aligned}
\alpha_{b_1}(k+1) - \alpha_{b_2}(k+1) &= b_1\alpha_{b_1}(k) - \alpha_{b_1}(k-1) - (b_2\alpha_{b_2}(k) - \alpha_{b_2}(k-1)) \\
&= b_1\alpha_{b_1}(k) - b_2\alpha_{b_2}(k) - (\alpha_{b_1}(k-1) - \alpha_{b_2}(k-1)).
\end{aligned}$$

Also, since $b_1 \equiv b_2 \bmod q$, there exist $a, i, j \in \mathbf{Z}$ such that $b_1 = iq + a$ and $b_2 = jq + a$,

so we get that

$$\begin{aligned}\alpha_{b_1}(k+1) - \alpha_{b_2}(k+1) &= (iq+a)\alpha_{b_1}(k) - (jq+a)\alpha_{b_2}(k) - (\alpha_{b_1}(k-1) - \alpha_{b_2}(k-1)) \\ &= iq\alpha_{b_1}(k) - jq\alpha_{b_2}(k) + a\alpha_{b_1}(k) - a\alpha_{b_2}(k) - (\alpha_{b_1}(k-1) - \alpha_{b_2}(k-1) \\ &= q(i\alpha_{b_1}(k) - j\alpha_{b_2}(k)) + a(\alpha_{b_1}(k) - \alpha_{b_2}(k)) - (\alpha_{b_1}(k-1) - \alpha_{b_2}(k-1)).\end{aligned}$$

By our induction hypothesis, we know that $\alpha_{b_1}(k) \equiv \alpha_{b_2}(k) \bmod q$, so $q|(\alpha_{b_1}(k) - \alpha_{b_2}(k))$, and $\alpha_{b_1}(k-1) \equiv \alpha_{b_2}(k-1) \bmod q$, so $q|(\alpha_{b_1}(k-1) - \alpha_{b_2}(k-1))$. Thus, there exist $r, s \in \mathbf{Z}$ such that

$$\begin{aligned}\alpha_{b_1}(k+1) - \alpha_{b_2}(k+1) &= q(i\alpha_{b_1}(k) - j\alpha_{b_2}(k)) + a(qr) - (qs) \\ &= q(i\alpha_{b_1}(k) - j\alpha_{b_2}(k) + ar - s).\end{aligned}$$

Thus, $q|(\alpha_{b_1}(k+1) - \alpha_{b_2}(k+1))$, so $\alpha_{b_1}(k+1) \equiv \alpha_{b_2}(k+1) \bmod q$. So, for all n, if $b_1 \equiv b_2 \bmod q$, then $\alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \bmod q$. □

Corollary 2.3.9. *For $b > 2$, $\alpha_b(n) \equiv n \bmod b-2$ for all n.*

Proof. Since $(b-2)|(b-2)$, it follows that $b \equiv 2 \bmod b-2$. Then, by Proposition 2.3.8, $\alpha_b(n) \equiv \alpha_2(n) \bmod b-2$, and further $\alpha_b(n) \equiv n \bmod b-2$ by Proposition 2.3.5. □

The nature of α_b as described by Proposition 2.3.8 and Corollary 2.3.9 will be of great importance in the following sections. We will also make use of the periodic nature of α_b, described by the following proposition.

Proposition 2.3.10. *For any positive integer v, α_b is periodic modulo v.*

In Section 3.1.3, the following proposition will be useful as well.

Proposition 2.3.11. *For all $b \geq 2$ and all n,*

$$(\alpha_b(n))^2 - \alpha_b(n+1)\alpha_b(n-1) = 1.$$

Proof. First, we use the elements of α_b to define a matrix A_b as follows:

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

with the convention that $\alpha_b(-1) = 0$. We start our proof by showing that

$$A_b(n) = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n.$$

Notice that

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

$$= \begin{pmatrix} b\alpha_b(n) - \alpha_b(n-1) & -\alpha_b(n) \\ b\alpha_b(n-1) - \alpha_b(n-2) & -\alpha_b(n-1) \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_b(n) & -\alpha_b(n-1) \\ \alpha_b(n-1) & -\alpha_b(n-2) \end{pmatrix} \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}$$

$$= A_b(n-1) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}.$$

For base cases, note that when $n = 0$,

$$A_b(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^0$$

and when $n = 1$,

$$A_b(1) = A_b(0) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^1.$$

For the induction case, assume that for all $n \leq k$

$$A_b(n) = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n.$$

We must show that

$$A_b(k+1) = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{k+1}.$$

By our induction hypothesis,

$$A_b(k+1) = A_b(k) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^k \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{k+1}.$$

Thus, by induction, for all n,

$$A_b(n) = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n.$$

Now, notice that

$$det\begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} = 1,$$

and since determinants are multiplicative,

$$det\left(A_b(n)\right) = det\left(\begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n\right) = 1^n = 1.$$

Also, using our original definition of $A_b(n)$, we get that

$$\begin{aligned} det\left(A_b(n)\right) &= \left(\alpha_b(n+1)\right)\left(-\alpha_b(n-1)\right) - \left(\alpha_b(n)\right)\left(-\alpha_b(n)\right) \\ &= \left(\alpha_b(n)\right)^2 - \alpha_b(n+1)\alpha_b(n-1) \end{aligned}$$

Thus we can conclude that

$$\left(\alpha_b(n)\right)^2 - \alpha_b(n+1)\alpha_b(n-1) = 1.$$

□

Lastly, in Section 2.3.4 we will use another characteristic of α_b, described below.

Corollary 2.3.12. *At least one of any two consecutive terms of α_b is odd.*

Proof. Suppose that both $\alpha_b(n)$ and $\alpha_b(n+1)$ are even. Then $\left(\alpha_b(n)\right)^2$ must be even, and $\alpha_b(n+1)\alpha_b(n-1)$ must be even as well. Then $\left(\alpha_b(n)\right)^2 - \alpha_b(n+1)\alpha_b(n-1) \geq 2$. But this is a contradiction to Proposition 2.3.11. Thus, at least one of $\alpha_b(n)$ and $\alpha_b(n+1)$ must be odd. □

We have now finished examining a number of characteristics of α_b that we will require in the following sections. With these characteristics in mind, we can move on to proving that the sets S and S_* are Diophantine.

2.3.3 S is a Diophantine Set.

In this section, we will prove that the set

$$S = \{< a, b > | b \geq 2 \text{ and } \exists n[a = \alpha_b(n)]\}$$

is a Diophantine set.

Lemma 2.3.13. *If $< a, b > \in S$, then the Diophantine equation $D(a, b, x) = x^2 - abx + a^2 - 1 = 0$ has a solution for x.*

Proof. Let $< a, b > \in S$. Then $b \geq 2$ and there exists an n such that $a = \alpha_b(n)$. Then let $x = \alpha_b(n-1)$. By Proposition 2.3.11, we know that $(\alpha_b(n))^2 - \alpha_b(n+1)\alpha_b(n-1) = 1$. Then we have that

$$\begin{aligned} D(a, b, x) &= (\alpha_b(n-1))^2 - b\alpha_b(n)\alpha_b(n-1) + (\alpha_b(n))^2 - 1 \\ &= (\alpha_b(n))^2 - b\alpha_b(n)\alpha_b(n-1) + (\alpha_b(n-1))^2 - 1 \\ &= (\alpha_b(n))^2 - (b\alpha_b(n) - \alpha_b(n-1))(\alpha_b(n-1)) - 1 \\ &= (\alpha_b(n))^2 - \alpha_b(n+1)\alpha_b(n-1) - 1 \\ &= 1 - 1 \\ &= 0. \end{aligned}$$

Therefore, when $< a, b > \in S$, the Diophantine equation $D(a, b, x) = x^2 - abx + a^2 - 1 = 0$ has a solution for x, namely $x = \alpha_b(n-1)$. □

Lemma 2.3.14. *For $b \geq 2$, if $x^2 - bxy + y^2 = 1$ and $y < x$, then there exists an m such that $x = \alpha_b(m+1)$ and $y = \alpha_b(m)$.*

Proof. Our proof will follow by induction on y.
For the base case, let $y = 0$.
Since $x^2 - bxy + y^2 = 1$, $x = 1$. For $m = 0$, $\alpha_b(0+1) = 1 = x$, and $\alpha_b(0) = 0 = y$, and thus our proposition holds.
For the induction case, fix $y > 0$, and assume that for any $\hat{y} < y$ and $\hat{x} > \hat{y}$, if $\hat{x}^2 - b\hat{x}\hat{y} + \hat{y}^2 = 1$, then there exists an $\hat{m}$ such that $\hat{x} = \alpha_b(\hat{m}+1)$ and $\hat{y} = \alpha_b(\hat{m})$.
Suppose that there is an $x > y$ such that $x^2 - bxy + y^2 = 1$. We need to find an m such that $y = \alpha_b(m)$ and $x = \alpha_b(m+1)$. Notice that

$$x = by + \left(\frac{1 - y^2}{x}\right) = by - \left(\frac{y^2 - 1}{x}\right) \leq by.$$

Further, since $x > y$, we know that $xy > y^2 > y^2 - 1$, and thus $y > \frac{y^2-1}{x}$. Then we get that

$$x = by \ + \ \left(\frac{1 - y^2}{x}\right) \ = \ by - \left(\frac{y^2 - 1}{x}\right) \ > \ by - y.$$

Now, define $x_1 = y$ and $y_1 = by - x$. Then since $x > by - y$, we get that

$$y_1 = by - x < by - (by - y) = y,$$

and further that

$$x_1 = y > y_1.$$

Also, notice that

$$\begin{aligned} x_1^2 - bx_1y_1 + y_1^2 &= y^2 - by(by - x) + (by - x)^2 \\ &= y^2 - b^2y^2 + bxy + b^2y^2 - 2bxy + x^2 \\ &= y^2 - bxy + x^2 \\ &= 1. \end{aligned}$$

Thus x_1 and y_1 are such that $y_1 < y$, $x_1 > y_1$, and $x_1^2 - bx_1y_1 + y_1^2 = 1$. Therefore by our induction hypothesis, there must exist some m_1 such that

$$x_1 = \alpha_b(m_1 + 1) \ \ and \ \ y_1 = \alpha_b(m_1).$$

Let $m = m_1 + 1$. Then

$$\begin{aligned} x &= by - y_1 \\ &= bx_1 - y_1 \\ &= b\alpha_b(m_1 + 1) - \alpha_b(m_1) \\ &= \alpha_b(m_1 + 2) \\ &= \alpha_b(m + 1) \end{aligned}$$

and

$$y = x_1 = \alpha_b(m_1 + 1) = \alpha_b(m).$$

Thus, by induction, for any $y \geq 0$ and $x > y$, if $x^2 - bxy + y^2 = 1$, then there must exist some m such that $x = \alpha_b(m + 1)$ and $y = \alpha_b(m)$. □

Theorem 2.3.15. *The set* $S = \{< a, b > | b \geq 2$ *and* $\exists n[a = \alpha_b(n)]\}$ *is a Diophantine set.*

Proof. It follows directly from Lemmas 2.3.13 and 2.3.14 that there exists a Diophantine equation, namely $D(a, b, x) = x^2 - bax + a^2$, such that $< a, b > \in S \iff D(a, b, x) = 0$ has solutions for x. Thus, by definition, S must be a Diophantine set. □

2.3.4 S_* is a Diophantine Set

In order to show that $S_* = \{< a, b, c > | a = \alpha_b(c)\}$ is a Diophantine set, we will find a system of Diophantine conditions that represents it. This system will be slightly harder to determine than the equation we used to represent S. Therefore, we will first work through the development of this system, before giving a formal proof that the system is solvable if and only if $< a, b, c > \in S_*$.

Determining the System of Diophantine Conditions

Step One:

First, we can consider S_* to be the union of the terms of the following sequence for all $b \geq 4$:

$$< \alpha_b(0), b, 0 >, ..., < \alpha_b(n), b, n >, ... \tag{2.3.1}$$

Step Two:

Next, we will rewrite Sequence 2.3.1 in such a way that n does not appear on its own, but rather only as an argument of α_b.

Proposition 2.3.16. *The first $b-2$ terms of 2.3.1 correspond to the first $b-2$ terms of the following sequence, for all $b \geq 4$:*

$$< \alpha_b(0), b, rem(\alpha_b(0), b-2) >, ..., < \alpha_b(n), b, rem(\alpha_b(n), b-2) >, ... \tag{2.3.2}$$

Proof. First, note that $n < b-2$ for the first $b-2$ terms of 2.3.1. By Corollary 2.3.9, we know that $\alpha_b(n) \equiv n \bmod b-2$. Therefore, when $n < b-2$, $rem(\alpha_b(n), b-2) = n$. □

Adjusting our sequence so that n only appears as an argument of α_b is particularly useful. Our only way to describe that a triple $< a, b, c >$ belongs to the set of elements of sequence 2.3.1 is with the conditions $b \geq 4$ and $a = \alpha_b(c)$, and we do not know that the latter condition is diophantine. However, we can say that a triple $< a, b, c >$ belongs to the set of elements of sequence 2.3.2 if $b \geq 4$ and $\exists n[a = \alpha_b(n)]$ and $c = rem(a, b-2)$, all of which we have seen are Diophantine conditions. The problem remains, however, that only the first $b-2$ members of 2.3.1 match 2.3.2.

Step Three:

Here again, we will adjust our initial sequence 2.3.1 by using three new variables, namely u, v, and w, and setting two conditions to be as follows:

$$Condition\ 1 : w \equiv b \bmod v$$

$$Conditon\ 2 : w \equiv 2 \bmod u.$$

Proposition 2.3.17. *If $w \equiv b \bmod v$ and $w \equiv 2 \bmod u$ and $v > 2\alpha_b(k)$ and $u > 2k$, then the first k entries of 2.3.1 correspond to the first k members of the following sequence for all $b \geq 4$:*

$$< arem(\alpha_b(0), v), b, arem(\alpha_b(0), u) >, ..., < arem(\alpha_b(n), v), b, arem(\alpha_b(n), u) >, ... \tag{2.3.3}$$

Proof. First, note that $n < k$ for the first k entries of 2.3.1. Let $w \equiv b \bmod v$. Then, from Proposition 2.3.8, we know that $\alpha_w(n) \equiv \alpha_b(n) \bmod v$. Also, let $v \geq 2\alpha_b(k)$. Then when $n < k$, $arem(\alpha_w(n), v) = \alpha_b(n)$. Further, let $w \equiv 2 \bmod u$. Then, from Proposition 2.3.8, we know that $\alpha_w(n) \equiv \alpha_2(n) \bmod u$, and thus by Proposition 2.3.5, $\alpha_w(n) \equiv n \bmod u$. Also, let $u > 2k$. Then, when $n < k$, $arem(\alpha_w(n), u) = n$. □

By requiring that $v > 2\alpha_b(k)$ and $u > 2k$, our new sequence again only matches sequence 2.3.1 for a finite number of terms. Therefore, rather than setting a particular k, we will require only that $w \equiv b \bmod v$ and $w \equiv 2 \bmod u$, and then take the union of all terms of any sequence of the form 2.3.3 such that u, v, and w satisfy these conditons. For each of these individual sequences in our union, there will be some $k \geq 0$ such that $v > 2\alpha_b(k)$ and $u > 2k$, and therefore each individual sequence will match sequence 2.3.1 for only k terms. However, since we are taking the union of all sequences of the form sequence 2.3.3 with all u, v and w satisfying $w \equiv b \bmod v$ and $w \equiv 2 \bmod u$, we can always find some $v_1 > v$ and some $u_1 > u$ such that that $k_1 > k$. Therefore, we can be certain that all triples from our original sequence 2.3.1 will be included in this union. However, our new set will contain extra triples as well, since for any individual sequence in our union, all of its terms will be included, not just the first k terms that match sequence 2.3.1. Therefore, our next goal will be to set additional conditions to eliminate these "extra" triples from our set.

Step Four:

First, we will narrow down the location of our "extra" triples by using Proposition 2.3.10, which states that for any positive v, the sequence $\alpha_b(0), ..., \alpha_b(n), ...$ is periodic mod v. Thus, we might predict that sequence 2.3.3 will be periodic as well. By choosing a specific v, we can control the length of this period, and thus narrow down the location of all unique triples to a finite initial segment of sequence 2.3.3. We will choose this v to be as follows:

$$Condition\ 3 : v = \alpha_b(m+1) - \alpha_b(m-1).$$

Let's start by finding the period of the sequence $arem(\alpha_w(0), v), ..., arem(\alpha_w(n), v), ...$ under this new condition on v.

Proposition 2.3.18. *If $v = \alpha_b(m+1) - \alpha_b(m-1)$, then the sequence $\alpha_b(0), ..., \alpha_b(n), ...,$ mod v has a period length of $4m$. In particular, the terms of the sequence will be as follows:*

n	$\alpha_b(n) \bmod v$
0	0
1	1
$\vdots$	$\vdots$
$m-1$	$\alpha_b(m-1)$
m	$\alpha_b(m)$
$m+1$	$\alpha_b(m-1)$
$\vdots$	$\vdots$
$2m-1$	1
$2m$	0
$2m+1$	-1
$\vdots$	$\vdots$
$3m-1$	$-\alpha_b(m-1)$
$3m$	$-\alpha_b(m)$
$3m+1$	$-\alpha_b(m-1)$
$\vdots$	$\vdots$
$4m-1$	-1

Proof. It is obvious that

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) \bmod v \\
\alpha_b(1) &\equiv \alpha_b(1) \bmod v \\
&\vdots \\
\alpha_b(m-1) &\equiv \alpha_b(m-1) \bmod v \\
\alpha_b(m) &\equiv \alpha_b(m) \bmod v
\end{aligned}$$

Since $v = \alpha_b(m+1) - \alpha_b(m-1)$, we have that

$$\alpha_b(m+1) \equiv \alpha_b(m-1) \bmod v.$$

From this, along with our original definition of α_b, and the equivalent definition of α_b given in Proposition 2.3.2,we get that

$$\begin{aligned}
\alpha_b(m+2) &= b\alpha_b(m+1) - \alpha_b(m) \\
&\equiv (b\alpha_b(m-1) - \alpha_b(m)) \bmod v \\
&\equiv \alpha_b(m-2) \bmod v
\end{aligned}$$

Continuing this process yields

$$\begin{aligned}
\alpha_b(m+3) &= b\alpha_b(m+2) - \alpha_b(m+1) \\
&\equiv (b\alpha_b(m-2) - \alpha_b(m-1)) \bmod v \\
&\equiv \alpha_b(m-3) \bmod v \\
&\vdots \\
\alpha_b(2m-1) &= \alpha_b(m+(m-1)) \\
&= b\alpha_b(m+(m-2)) - \alpha_b(m+(m-3)) \\
&\equiv (b\alpha_b(m-(m-2)) - \alpha_b(m-(m-3))) \bmod v \\
&\equiv (b\alpha_b(2) - \alpha_b(3)) \bmod v \\
&\equiv \alpha_b(1) \bmod v \\
&\equiv 1 \bmod v
\end{aligned}$$

$$\begin{aligned}
\alpha_b(2m) &= \alpha_b(m+m) \\
&= b\alpha_b(m+(m-1)) - \alpha_b(m+(m-2)) \\
&\equiv (b\alpha_b(m-(m-1)) - \alpha_b(m-(m-2))) \bmod v \\
&\equiv (b\alpha_b(1) - \alpha_b(2)) \bmod v \\
&\equiv \alpha_b(0) \bmod v \\
&\equiv 0 \bmod v
\end{aligned}$$

$$\begin{aligned}
\alpha_b(2m+1) &= \alpha_b(m+(m+1)) \\
&= b\alpha_b(m+m) - \alpha_b(m+(m-1)) \\
&\equiv (b\alpha_b(m-m) - \alpha_b(m-(m-1))) \bmod v \\
&\equiv (b\alpha_b(0) - \alpha_b(1)) \bmod v \\
&\equiv -\alpha_b(1) \bmod v \\
&\equiv -1 \bmod v
\end{aligned}$$

To continue past $\alpha_b(2m+1)$, we will show by induction that for all $n \geq 2$,

$$\alpha_b(2m+n) \equiv -\alpha_b(n) \bmod v.$$

For a base case, let $n = 2$. We have seen that

$$\alpha_b(2m) \equiv 0 \equiv -\alpha_b(2m) \bmod v$$

and that

$$\alpha_b(2m+1) \equiv -1 \equiv -\alpha_b(2m-1) \bmod v.$$

Thus,

$$\begin{aligned}
\alpha_b(2m+2) &= b\alpha_b(2m+1) - \alpha_b(2m) \text{ by the definition of } \alpha_b \\
&\equiv -b\alpha_b(2m-1) - (-\alpha_b(2m)) \bmod v \\
&\equiv -(b\alpha_b(2m-1) - \alpha_b(2m)) \bmod v \\
&\equiv -\alpha_b(2m-2) \bmod v \text{ by Proposition 2.3.2} \\
&\equiv -\alpha_b(m+(m-2)) \bmod v \\
&\equiv -\alpha_b(m-(m-2)) \bmod v \text{ by the initial part of this proof} \\
&\equiv -\alpha_b(2) \bmod v
\end{aligned}$$

Now for the induction case, assume that for all $n \leq k$ that

$$\alpha_b(2m+n) \equiv -\alpha_b(2m-n) \equiv -\alpha_b(n) \bmod v.$$

We must show that

$$\alpha_b(2m+(k+1)) \equiv -\alpha_b(2m-(k+1)) \equiv -\alpha_b(k+1) \bmod v.$$

We find that

$$\begin{aligned}
\alpha_b(2m+(k+1)) &= b\alpha_b(2m+k) - \alpha_b(2m+(k-1)) \text{ by the definition of } \alpha_b \\
&\equiv -b\alpha_b(2m-k) - (-\alpha_b(2m-(k-1))) \bmod v \text{ by our induction hypothesis} \\
&\equiv -(b\alpha_b(2m-k) - \alpha_b(2m-(k-1))) \bmod v \\
&\equiv -\alpha_b(2m-(k+1)) \bmod v \text{ by Proposition 2.3.2} \\
&\equiv -\alpha_b(m+(m-k-1)) \bmod v \\
&\equiv -\alpha_b(m-(m-k-1)) \bmod v \text{ by the initial part of this proof} \\
&\equiv -\alpha_b(k+1) \bmod v
\end{aligned}$$

as desired.

Using the fact that $\alpha_b(2m+n) \equiv -\alpha_b(n) \bmod v$ for any n, we can now calculate

the rest of the terms of $\alpha_b \bmod v$ to be as follows:

$$\begin{aligned}
&\alpha_b(2m+1) \equiv -1 \bmod v \\
&\qquad\qquad \vdots \\
&\alpha_b(3m-1) \equiv \alpha_b(2m+(m-1)) \equiv -\alpha_b(m-1) \bmod v \\
&\alpha_b(3m) \equiv \alpha_b(2m+(m)) \equiv -\alpha_b(m) \bmod v \\
&\alpha_b(3m+1) \equiv \alpha_b(2m+(m+1)) \equiv -\alpha_b(m+1) \equiv -\alpha_b(m-1) \bmod v \\
&\qquad\qquad \vdots \\
&\alpha_b(4m-1) \equiv \alpha_b(2m+(2m-1)) \equiv -\alpha_b(2m-1) \equiv -1 \bmod v \\
&\alpha_b(4m) \equiv \alpha_b(2m+2m) \equiv -\alpha_b(2m) \equiv 0 \bmod v \\
&\alpha_b(4m+1) \equiv \alpha_b(2m+(2m+1)) \equiv -\alpha_b(2m+1) \equiv -(-1) \equiv 1 \bmod v \\
&\qquad\qquad \vdots
\end{aligned}$$

At $\alpha_b(4m)$ we can see that the terms of $\alpha_b \bmod v$ begin to repeat, resulting in a period length of $4m$. □

Corollary 2.3.19. *If $w \equiv b \bmod v$ and $v = \alpha_b(m+1) - \alpha_b(m-1)$, then the sequence $\alpha_w \bmod v$ has period $4m$, with the same terms as the sequence $\alpha_b \bmod v$.*

Proof. Since $w \equiv b \bmod v$, by Proposition 2.3.8, we know that $\alpha_b(n) \equiv \alpha_w(n) \bmod v$. □

Corollary 2.3.20. *If $w \equiv b \bmod v$ and $v = \alpha_b(m+1) - \alpha_b(m-1)$, then the sequence $arem(\alpha_w(0), v), ..., arem(\alpha_w(n), v), ...$ has period $2m$. In particular, the sequence will be as follows:*

n	$arem(\alpha_w(n), v)$
0	0
1	1
$\vdots$	$\vdots$
$m-1$	$\alpha_b(m-1)$
m	$\alpha_b(m)$
$m+1$	$\alpha_b(m-1)$
$\vdots$	$\vdots$
$2m-1$	1

Proof. First, notice that

$$\begin{aligned} v &= \alpha_b(m+1) - \alpha_b(m-1) \\ &= (b\alpha_b(m) - \alpha_b(m-1)) - \alpha_b(m-1) \\ &= b\alpha_b(m) - 2\alpha_b(m-1). \end{aligned}$$

Then since $b \geq 4$ and $\alpha_b(m) > \alpha_b(m-1)$ by Proposition 2.3.3, we get that

$$v \geq 2\alpha_b(m).$$

Then Corollary 2.3.20 follows from Corollary 2.3.19 and the definition of the *arem* function. □

We have now found the period of the sequence $arem(\alpha_w(0), v), ..., arem(\alpha_w(n), v), ...$, whose elements are the first terms in the triples of sequence 2.3.3. Next, let's find the period of the sequence $arem(\alpha_w(0), u), ..., arem(\alpha_w(n), u), ...$, whose elements are the third terms in the triples of sequence 2.3.3. We will begin with the following proposition.

Proposition 2.3.21. *If $w \equiv 2 \bmod u$, then the sequence $\alpha_w(0), ..., \alpha_w(n), ..., \bmod u$ has a period of length u. In particular, the terms of the sequence will be as follows:*

n	$\alpha_w(n) \bmod u$
0	0
1	1
⋮	⋮
$u-1$	$u-1$

Proof. Since $w \equiv 2 \bmod u$, we know that $\alpha_w(n) \equiv \alpha_w(2) \bmod u$ by Proposition 2.3.8. Then by Proposition 2.3.5, we can conclude that $\alpha_w(n) \equiv n \bmod u$. □

Corollary 2.3.22. *If $w \equiv 2 \bmod u$, then the sequence $arem(\alpha_w(0), u), ..., arem(\alpha_w(n), u), ...$ has a period length of u. In particular, the terms of the sequence will be*

n	$arem(\alpha_w(n), u)$
0	0
1	1
$\vdots$	$\vdots$
$\frac{u}{2} - 1$	$\frac{u}{2} - 1$
$\frac{u}{2}$	$\frac{u}{2}$
$\frac{u}{2} + 1$	$\frac{u}{2} - 1$
$\vdots$	$\vdots$
$u - 1$	1
u	0

for even u, and

n	$arem(\alpha_w(n), u)$
0	0
1	1
$\vdots$	$\vdots$
$\frac{u-1}{2} - 1$	$\frac{u-1}{2} - 1$
$\frac{u-1}{2}$	$\frac{u-1}{2}$
$\frac{u-1}{2} + 1$	$\frac{u-1}{2} - 1$
$\vdots$	$\vdots$
$u - 1$	1
u	0

for odd u.

Proof. For $n = 0$ to $n = \frac{u}{2}$, $n \leq \frac{u}{2}$, so $arem(\alpha_w(n), u) = n$. For $n = \frac{u}{2} + 1$ to $n = u$,

$n > \frac{u}{2}$, so $arem(\alpha_w(n)) = u - n$. Thus we see that

$$\begin{aligned} arem\left(\alpha_w\left(\frac{u}{2}+1\right), u\right) &= u - \left(\frac{u}{2}+1\right) = \frac{u}{2} - 1 \\ &\vdots \\ arem(\alpha_w(u-1), u) &= u - (u-1) = 1 \\ arem(\alpha_w(u), u) &= u - u = 0 \end{aligned}$$

□

Now that we have examined the periods of the terms of the triples in sequence 2.3.3, we can examine the period of the entire sequence. First, we will add a new condition on u, namely

$$Condition\ 4 : u|m.$$

With the addition of this condition, we arrive at the following theorem.

Proposition 2.3.23. *If $w \equiv b \bmod v$, $w \equiv 2 \bmod u$, $v = \alpha_b(m+1) - \alpha_b(m-1)$ and $u|m$, then sequence 2.3.3 has a period length of $2m$. In particular, the terms of sequence 2.3.3 will be as follows:*

n	$< arem(\alpha_w(n), v), b, arem(\alpha_w(n), u) >$
0	$< 0, b, 0 >$
1	$< 1, b, 1 >$
$\vdots$	$\vdots$
$\frac{u}{2} - 1$	$< \alpha_b(\frac{u}{2} - 1), b, \frac{u}{2} - 1 >$
$\frac{u}{2}$	$< \alpha_b(\frac{u}{2}), b, \frac{u}{2} >$
$\frac{u}{2} + 1$	$< \alpha_b(\frac{u}{2} + 1), b, \frac{u}{2} - 1 >$
$\vdots$	$\vdots$
$u - 1$	$< \alpha_b(u - 1), b, 1 >$
u	$< \alpha_b(u), b, 0 >$
$u + 1$	$< \alpha_b(u + 1), b, 1 >$
$\vdots$	$\vdots$
$m - 1$	$< \alpha_b(m - 1), b, 1 >$
m	$< \alpha_b(m), b, 0 >$
$m + 1$	$< \alpha_b(m - 1), b, 1 >$
$\vdots$	$\vdots$
$\vdots$	$\vdots$
$\vdots$	$\vdots$
$2m - 1$	$< 1, b, 1 >$

Proof. From Corollary 2.3.20, we know that $arem(\alpha_w(0), v), ..., arem(\alpha_w(n), v), ...$ has a period length of $2m$, and from Corollary 2.3.22, we know that $arem(\alpha_w(0), u), ...,$ $arem(\alpha_w(n), u), ...$ has a period length of u. Then since $u|m$, we know that $u|2m$,and thus the period of $arem(\alpha_w(0), u), ..., arem(\alpha_w(n), u), ...$ fits into the period of $arem(\alpha_w(0), v), ..., arem(\alpha_w(n), v), ...$ Putting these terms together in the triples of 2.3.3 therefore yields a sequence with a period of $2m$. The specific terms of 2.3.3 follow directly from Corrolaries 2.3.20 and 2.3.22 as well. □

Corollary 2.3.24. *If $w \equiv b \bmod v$, $w \equiv 2 \bmod u$, $v = \alpha_b(m + 1) - \alpha_b(m - 1)$ and $u|m$, then the "extra" triples of sequence 2.3.3 can be found in its first $m + 1$ entries.*

Proof. From the specifc terms of $arem(\alpha_w(0), v), ..., arem(\alpha_w(n), v), ...$ given in Corollary 2.3.20, and the specific terms of $arem(\alpha_w(0), u), ..., arem(\alpha_w(n), u), ...$ given in Corollary 2.3.22, we can see that both sequences are symmetric. Thus, the unique terms of sequence $arem(\alpha_w(0), v), ..., arem(\alpha_w(n), v), ...$ can be found in its first $m+1$ terms, and the unique terms of $arem(\alpha_w(0), u), ..., arem(\alpha_w(n), u), ...$ can be found

in its first $u/2+1$ terms. Since $u|m$, 2.3.3 will be symmetric as well, with its unique terms located within the first $m+1$ elements. □

Now that we have located the "extra" triples, we just need to determine condition(s) to eliminate these triples from our set.

Step Five:

To eliminate the extra triples, we will require that

$$Condition\ 5 : 2arem(\alpha_w(n), v) < u.$$

Proposition 2.3.25. *The conditions that $v = \alpha_b(m+1) - \alpha_b(m-1)$, $u|m$, and $2arem(\alpha_w(n), v) < u$ eliminate the "extra" triples from our set.*

Proof. Recall that

$$\begin{aligned} v &= \alpha_b(m+1) - \alpha_b(m-1) \\ &= ((b\alpha_b(m) - \alpha_b(m-1)) - \alpha_b(m-1) \\ &= b\alpha_b(m) - 2\alpha_b(m-1) \\ &\geq 2\alpha_b(m) \end{aligned}$$

Thus when $n < m+1$, $arem(\alpha_w(n), v) = \alpha_b(n)$. Since all the extra triples are located within the first $m+1$ terms of 2.3.3, the condition $2arem(\alpha_w(n), v) < u$ can be rewritten as $2\alpha_b(n) < u$. Then by Proposition 2.3.3, we know that $n < \alpha_b(n)$, and therefore $2n < u$. This implies by Corollary 2.3.22 that $arem(\alpha_w(n), u) = n$. Thus, the conditions that we implemented do in fact ensure that $arem(\alpha_w(n), u) = n$ and $arem(\alpha_w(n), v) = \alpha_b(n)$. □

By eliminating these extra triples, we have now constructed a set that is equivalent to the set of elements of sequence 2.3.1.

Step Six:

The previous steps have given us a set of conditions that can be used represent the set of elements of sequence 2.3.1. The only thing left to do is check that these conditions are Diophantine. In Example 2.1.4, we saw that the equivalence relation is Diophantine, and thus we know that Condition 1 and Condition 2 are Diophantine conditions. Also, in Example 2.2.1, we saw that the *arem* function is Diophantine, and thus we know that Condition 5 is Diophantine as well. A slight problem occurs, however, with Condtions 3 and 4, as we do not know that the condition $u|m$ together with $v = \alpha_b(m+1) = \alpha_b(m-1)$ is Diophantine. From the previous section, we know

that the conditions $s^2 - bsr + r^2 = 1$ together with $r < s$ are Diophantine conditions that imply that $\exists m[s = \alpha_b(m)\ and\ r = \alpha_b(m-1)]$. Thus we can express the condition $v = \alpha_b(m+1) - \alpha_b(m-1) = b\alpha_b(m) - 2\alpha_b(m-1)$ in a diophantine way with the condtions $s^2 - bsr + r^2 = 1$, $r < s$, and $v = bs - 2r$. However, we can only ensure the existance of m; we cannot set any conditions on m itself in a Diophantine way. Thus we cannot guarantee that the condition $u|m$ is Diophantine. In order to fix this problem, we will use the following proposition.

Proposition 2.3.26. *If $(\alpha_b(k))^2|\alpha_b(m)$, then $\alpha_b(k)|m$.*

Proof. Suppose that $\alpha_b(k)^2 \mid \alpha_b(m)$. If $\alpha_b(m) = 0$, then $m = 0$, so $\alpha_b(k)|m$.Then assume that $\alpha_b(m) \neq 0$. Then since $\alpha_b(k)^2 \mid \alpha_b(m)$, $\alpha_b(k) < \alpha_b(m)$, so $k < m$. Then by the division algorithm, we know that we can find some l and n such that

$$m = kl + n\ 0 \leq n < k$$

. Recall from the proof of Proposition 2.3.11 that we can define the matrix A_b whose elements are defined by α_b and for any x, $A_b(x) = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^x$. Then we find that

$$\begin{aligned} A_b(m) &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^m \\ &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{n+kl} \\ &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{kl} \\ &= A_b(n) \cdot A_b(k)^l \end{aligned}$$

Plugging in for each matrix, we find that

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \cdot \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^l.$$

Then it follows that

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \cdot \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^l \bmod (\alpha_b(k)).$$

Then considering this congruence element-wise, we find that

$$\alpha_b(m) \equiv \alpha_b(n) \cdot \alpha_b(k+1)^l - \alpha_b(n-1) \cdot 0 \equiv \alpha_b(n) \cdot \alpha_b(k+1)^l \bmod (\alpha_b(k)).$$

Therefore,

$$\alpha_b(k) \mid (\alpha_b(m) - \alpha_b(n)\alpha_b(k+1)^2).$$

Now, suppose that there is some d such that $d|\alpha_b(k)$ and $d|\alpha_b(k+1)$. Recall that by Proposition 2.3.11,

$$\alpha_b(k)^2 - \alpha_b(k+1)\alpha_b(k-1) = 1.$$

Then $d|1$, so $d = 1$. Therefore, we know that $\alpha_b(k)$ and $\alpha_b(k+1)$ are coprime. Putting this together with the fact that $\alpha_b(k) \mid (\alpha_b(m) - \alpha_b(n)\alpha_b(k+1)^2)$, we find that

$$\alpha_b(k) \mid \alpha_b(n).$$

However, we also know that $n < k$, and therefore by Proposition 2.3.3,

$$\alpha_b(n) < \alpha_b(k).$$

So, $\alpha_b(n) = 0$, meaning $n = 0$, and $m = kl$. With this, we find that

$$A_b(n) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

. Then it follows that

$$\begin{aligned} A_b(m) &= [A_b(k)]^l \\ &= \left[\begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}\right]^l \\ &= \left[\begin{pmatrix} \alpha_b(k)b & -\alpha_b(k) \\ \alpha_b(k) & 0 \end{pmatrix} - \begin{pmatrix} \alpha_b(k-1) & 0 \\ 0 & \alpha_b(k-1) \end{pmatrix}\right]^l \\ &= \left[\alpha_b(k)\begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} - \alpha_b(k-1)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]^l \\ &= \sum_{i=0}^{l} (-1)^{l-i}\binom{l}{i}\alpha_b(k)^i\alpha_b(k-1)^{l-i}\begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^i \end{aligned}$$

Then if we consider this equivalence $\bmod \alpha_b(k)^2$, all terms in the summation become 0 except for those with $i = 0$ and $i = 1$. Thus

$$A_b(m) = \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix}$$

$$\equiv (-1)^l \alpha_b(k-1)^l \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (-1)^{l-1} l \alpha_b(k) \alpha_b(k-1)^{l-1} \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \bmod (\alpha_b(k)^2).$$

Then if we consider this congruence element-wise, we find that

$$\alpha_b(m) \equiv (-1)^{l-1} l \alpha_b(k) \alpha_b(k-1)^{l-1} \bmod (\alpha_b(k)^2)$$

and thus that

$$\alpha_b(k)^2 \mid \left[\alpha_b(m) - \left[(-1)^{l-1} l \alpha_b(k) \alpha_b(k-1)^{l-1}\right]\right].$$

Then since we know also that $\alpha_b(k)^2 \mid \alpha_b(m)$, we find that

$$\alpha_b(k)^2 \mid l \alpha_b(k) \alpha_b(k-1)^{l-1},$$

meaning

$$\alpha_b(k) \mid l \alpha_b(k-1)^{l-1}.$$

Now, again by Proposition 2.3.11, we know that

$$\alpha_b(k)^2 - \alpha_b(k+1)\alpha_b(k-1) = 1$$

and thus $\alpha_b(k)$ and $\alpha_b(k-1)$ are coprime by the same reasoning used to show that $\alpha_b(k)$ and $\alpha_b(k+1)$ are coprime. Thus, it follows that

$$\alpha_b(k) \mid l,$$

and since $m = lk$,

$$\alpha_b(k) \mid \alpha_b(m)$$

as desired. □

Therefore, we can use the diophantine condition that $u^2 - but + t^2 = 1$ to guarantee that $\exists k[u = \alpha_b(k)]$ and then set the Diophantine condition that $u^2|s$, where $s = \alpha_b(m)$ for some m.

We are now prepared to give a formal proof that S_* is a Diophantine set.

Formal Proof

Lemma 2.3.27. *Given a,b,c, suppose there exist s, r, u, t, v, w such that the following conditions hold:*

$$\begin{aligned} b &\geq 4, \\ u^2 - but + t^2 &= 1 \\ s^2 - bsr + r^2 &= 1 \\ r &< s \\ u^2 &| s \\ v &= bs - 2r \\ v &| w - b \\ u &| w - 2 \\ w &> 2 \\ x^2 - wxy + y^2 &= 1 \\ 2a &< u \\ a &= arem(x, v) \\ c &= arem(x, u). \end{aligned}$$

Then $a = \alpha_b(c)$.

Proof. First, by Section 2.3.3, we know that

$$\left.\begin{aligned} b &\geq 4 \\ u^2 - but + t^2 &= 1 \end{aligned}\right\} \exists k[u = \alpha_b(k)]$$

Likewise, by Section 2.3.3, we know that

$$\left.\begin{aligned} b &\geq 4 \\ r &< s \\ s^2 - bsr + r^2 &= 1 \end{aligned}\right\} \exists m[s = \alpha_b(m) \text{ and } r = \alpha_b(m-1)]$$

Also, by Proposition 2.3.26, we have that

$$\left.\begin{aligned} u^2 &| s \\ u &= \alpha_b(k) \\ s &= \alpha_b(m) \end{aligned}\right\} u | m$$

Next, by Definition 2.3.1, we get that

$$\left.\begin{array}{l} v = bs - 2r \\ s = \alpha_b(m) \\ r = \alpha_b(m-1) \end{array}\right\} v = b\alpha_b(m) - 2\alpha_b(m-1) = \alpha_b(m+1) - \alpha_b(m-1)$$

Further, by Section 2.3.3, we know that

$$\left.\begin{array}{c} w > 2 \\ x^2 - wxy + y^2 = 1 \end{array}\right\} \exists n[x = \alpha_w(n)]$$

Next, note that the condition $v|(w-b)$ implies that $w \equiv b \bmod v$ and the condition $u|(w-2)$ implies that $w \equiv 2 \bmod u$. Therefore, by Propositions 2.3.5 and 2.3.8, we get that

$$\left.\begin{array}{l} x = \alpha_w(n) \\ v|(w-b) \\ u|(w-2) \end{array}\right\} x \equiv \alpha_b(n) \bmod v \text{ and } x \equiv n \bmod u$$

Now, note that for any n and m, we can let

$$n = 2lm \pm j \text{ with } j \leq m$$

for some l and j.In particular, this is always possible because we allow that $l = 0$. Given this, we can now show that

$$x \equiv \alpha_b(n) \equiv \pm\alpha_b(j) \bmod v.$$

First, recall that we can define the matrix $A_b(n)$ using α_b as follows:

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

Further, recall that in the proof of Proposition 2.3.11, we found that

$$A_b(n) = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n$$

Then given that $n = 2lm \pm j$, we find that

$$\begin{aligned} A_b(n) &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n \\ &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{2lm \pm j} \\ &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{m2l} \cdot \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{\pm j} \\ \\ &= A_b(m)^{2l} \cdot A_b(j)^{\pm 1} \end{aligned}$$

Further, because we know that $v = \alpha_b(m+1) - \alpha_b(m-1)$, we know that $v|(\alpha_b(m+1) - \alpha_b(m-1))$, meaning $\alpha_b(m+1) \equiv \alpha_b(m-1) \bmod v$. Therefore,

$$\begin{aligned} A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\ \\ &\equiv \begin{pmatrix} \alpha_b(m-1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m+1) \end{pmatrix} \bmod v \\ \\ &\equiv - \begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} \bmod v \end{aligned}$$

Now, suppose we attempted to find the inverse of $A_b(m)$, i.e the matrix $\begin{pmatrix} d & f \\ g & h \end{pmatrix}$ such that

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \cdot \begin{pmatrix} d & f \\ g & h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then we end up with the system of equations

$$\begin{aligned} \alpha_b(m+1)d - \alpha_b(m)g &= 1 \\ \alpha_b(m)d - \alpha_b(m-1)g &= 0 \\ \alpha_b(m+1)f - \alpha_b(m)h &= 0 \\ \alpha_b(m)f - \alpha_b(m-1)h &= 1 \end{aligned}$$

which we can solve to find that

$$\begin{aligned} d &= -\alpha_b(m-1) \\ f &= \alpha_b(m) \\ g &= -\alpha_b(m) \\ h &= \alpha_b(m+1) \end{aligned}$$

meaning

$$A_b(m)^{-1} = \begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix}.$$

Putting this together with our previous result, we now have that

$$A_b(m) \equiv -A_b(m)^{-1} \bmod v$$

and thus

$$A_b(m)^2 \equiv -A_b(m)^{-1}A_b(m) \equiv -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod v.$$

Putting this together with our result that

$$A_b(n) = A_b(m)^{2l} \cdot A_b(j)^{\pm 1},$$

we find that

$$A_b(n) \equiv \pm A_b(j)^{\pm 1} \bmod v$$

where all four combinations of the $+$ and $-$ signs are possible. Then examining this congruence element-wise, we find that

$$x \equiv \alpha_b(n) \equiv \pm\alpha_b(j) \bmod v,$$

as desired.
Next, we can examine the following sequence of inequalities to find that $2\alpha_b(j) \leq v$:

$$\begin{aligned} 2\alpha_b(j) &\leq 2\alpha_b(m) \text{ since } j \leq m \\ &\leq (b-2)\alpha_b(m) \text{ since } b \geq 4 \\ &= b\alpha_b(m) - 2\alpha_b(m) \\ &< b\alpha_b(m) - 2\alpha_b(m-1) \text{ since } \alpha_b \text{ is increasing} \\ &= v \end{aligned}$$

Therefore, we now have that

$$\left.\begin{array}{l} 2\alpha_b(j) < v \\ a = arem(x, v) \\ x \equiv \alpha_b(n) \bmod v \end{array}\right\} a = arem(x, v) = arem(\alpha_b(n), v) = \alpha_b(j)$$

Then, with this result and the fact that α_b , we have that

$$\left.\begin{array}{l} a = \alpha_b(j) \\ 2a < u \end{array}\right\} 2j \leq 2\alpha_b(j) = 2a < u$$

With this, we have that

$$\left.\begin{array}{l} c = arem(x, u) \\ x \equiv n \bmod u \\ n = 2lm \pm j \\ u|m \\ 2j < u \end{array}\right\} c = arem(x, u) = arem(n, u) = j$$

And finally, we arrive at our desired result, as

$$\left.\begin{array}{l} a = \alpha_b(j) \\ c = j \end{array}\right\} a = \alpha_b(c)$$

□

Lemma 2.3.28. *Let $a = \alpha_b(c)$ and $b \geq 4$. Then there exist s, r, u, t, v, w such that:*

$$\begin{aligned} u^2 - but + t^2 &= 1 \\ s^2 - bsr + r^2 &= 1 \\ r &< s \\ u^2 &| s \\ v &= bs - 2r \\ v &| w - b \\ u &| w - 2 \\ w &> 2 \\ x^2 - wxy + y^2 &= 1 \\ 2a &< u \\ a &= arem(x, v) \\ c &= arem(x, u). \end{aligned}$$

Proof. First, we choose u such that $u = \alpha_b(k)$ for some k, u is odd, and $2a < u$. We can guarantee that we can find such a u, because by Proposition 2.3.3, we know that α_b is an increasing sequence, and by Corollary 2.3.12, we know that at least one of any two consecutive terms of α_b is odd.

Next, we let $t = \alpha_b(k+1)$. Then by Section 2.3.3, we know that the condition

$$u^2 - but + t^2 = 1$$

holds.

Further, we let $m = uk$, and choose r and s such that $s = \alpha_b(m)$ and $r = \alpha_b(m-1)$. Then by Proposition 2.3.3 and Section 2.3.3, we know that the conditions

$$s^2 - bsr + r^2 = 1 \text{ and } r < s$$

both hold.

Then by the proof of Proposition 2.3.26, we find that

$$s = \alpha_b(uk) \equiv (-1)^{u-1} u\alpha_b(k)\alpha_b(k-1)^{u-1} \bmod (\alpha_b(k)^2).$$

Since u is odd, $u-1$ is even, meaning $(-1)^{u-1} = 1$. Further, since $u = \alpha_b(k)$, we have that

$$s \equiv u^2\alpha_b(k-1)^{u-1} \bmod u^2,$$

and thus the condition $u^2 \mid s$ must hold.

Next, since we know that $s = \alpha_b(m)$ and $r = \alpha_b(m-1)$, we can find that

$$\begin{aligned} bs - 2r &= b\alpha_b(m) - 2\alpha_b(m-1) \\ &\geq 4\alpha_b(m) - 2\alpha_b(m-1) \\ &> 4\alpha_b(m) - 2\alpha_b(m) \\ &= 2\alpha_b(m) > 0 \end{aligned}$$

so we can choose $v = bs - 2r$.

Next, we'll guarantee that there is some w that satisfies the conditions $w > 2$, $v|w-b$, and $u|w-2$. In particular, this requires that the system $w \equiv b \bmod v$ and $w \equiv u \bmod u$ has a solution for w. By the Chinese Remainder Theorem, we know that such a solution exists as long as u and v are coprime. To check that this is in fact the case, suppose that there is some d such that $d|u$ and $d|v$. Since $u^2|s$, it follows that $d|s$. Since $v = bs - 2r$, $d|2r$, and since u is odd, d is odd, so $d|r$. Therefore, since $s^2 - bsr + r^2 = 1$, $d|1$, so $d = 1$. Therefore, u and v are in fact coprime.

Further, we can choose x and y such that $x = \alpha_w(c)$ and $y = \alpha_w(c+1)$. Then by Section 2.3.3, we know that the condition

$$x^2 - wxy + y^2 = 1$$

holds.

Next, by the condition $v|w - b$, we know that $w \equiv b \bmod v$, and therefore by Proposition 2.3.8, we know that $\alpha_w(c) \equiv \alpha_b(c) \bmod v$. Then since $a = \alpha_b(c)$ and $x = \alpha_w(c)$, we find that $x \equiv a \bmod v$. Also, above we saw that $v > 2\alpha_b(m)$. Then $2a < u$ and $m = uk$, we know that $a < m < \alpha_b(m)$, meaning $v > 2a$. Thus, we can conclude that $a = arem(x, v)$.

Lastly, since $w > 2$, we know by Corollary 2.3.9 that $x = \alpha_w(c) \equiv c \bmod w - 2$. Then since $u|w - 2$, $x \equiv c \bmod u$. Further, we know that $2c \leq 2\alpha_b(c) = 2a \leq u$. Therefore, we can conclude that $c = arem(x, u)$.

□

Theorem 2.3.29. *S_* is a Diophantine set.*

Proof. Since all conditions stated in Proposition 2.3.27 and 2.3.28 are Diophantine conditions, these two propositions together prove that S^* is a Diophantine set. □

2.3.5 The set $\{< a, b, c > | a = b^c\}$ is Diophantine

We have now completed our analysis of of α_b, with the important result that $S_* = \{< a, b, c > | a = \alpha_b(c)\}$ is a Diophantine set. In this section, we will compare S_* to the set $\{< a, b, c > | a = b^c\}$. In particular, we will attempt to rewrite b^c in terms of α_b, and thus prove that exponentiation is Diophantine. For convenience, we will define $0^0 = 1$ throughout this section.

We will begin our comparison with the following proposition.

Proposition 2.3.30. $(b-1)^n \leq \alpha_b(n+1) \leq b^n$

Proof. Our proof will proceed by induction.
Let $n = 0$. Then $(b-1)^n = 1$, $\alpha_b(n+1) = 1$, and $b^n = 1$, and since $1 \leq 1 \leq 1$, the proposition holds. Let $n = 1$. Then $(b-1)^n = b - 1$, $\alpha_b(n+1) = b$, and $b^n = b$, and since $b - 1 \leq b \leq b$, the proposition holds. For the induction case, assume $(b-1)^n \leq \alpha_b(n+1) \leq b^n$ for all $n \leq k$. We must show that $(b-1)^{k+1} \leq \alpha_b(k+1+1) \leq b^{k+1}$. By our induction hypothesis, we know that

$$\alpha_b(k+1) \leq b^k$$

and so

$$b \cdot \alpha_b(k+1) \leq b \cdot b^k,$$

meaning

$$b \cdot \alpha_b(k+1) - \alpha_b(k) \leq b \cdot b^k.$$

Thus,

$$\alpha_b(k+2) \leq b^{k+1}.$$

Also, by our induction hypothesis we know that

$$(b-1)^k \leq \alpha_b(k+1)$$

and therefore

$$(b-1) \cdot (b-1)^k \leq (b-1) \cdot \alpha_b(k+1) = b\alpha_b(k+1) - \alpha_b(k+1).$$

Then since α_b is increasing, we know that

$$(b-1) \cdot (b-1)^k \leq b\alpha_b(k+1) - \alpha_b(k),$$

meaning

$$(b-1)^{k+1} \leq \alpha_b(k+2).$$

Thus, we have found that

$$(b-1)^{k+1} \leq \alpha_b(k+2) \leq b^{k+1}.$$

This implies, by induction, that for all $n \geq 0$,

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n.$$

□

Next, we will prove a similar but slightly more complex inequality. Although it may seem strange at first, it will actually be quite useful in developing a Diophantine way to express b^c in terms of α_b.

Proposition 2.3.31. *For all $b \geq 0$ and all $c \geq 0$, if $x > 16(c+1)(b+1)^c$,then*

$$b^c \leq \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} < b^c + 1.$$

Proof. First, we note that since $x > 16(c+1)(b+1)^c$, $x \geq 16$. Our proof will be split into two cases, one for $b = 0$, and one for $b > 0$.

Case 1: Let $b = 0$.
Say $c = 0$. Then for any x,

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} = \frac{\alpha_{bx+4}(1)}{\alpha_x(1)} = \frac{1}{1} = 1.$$

Then since we have defined $0^0 = 1$, we obtain that

$$1 \ \leq \ \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \ < \ 2,$$

and thus our proposition holds.
Then instead say $c > 0$. By Proposition 2.3.30, we know that

$$\alpha_{bx+4}(c+1) \ \leq \ (bx+4)^c = 4^c$$

and

$$\alpha_x(c+1) \ \geq \ (x-1)^c,$$

and therefore

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \ \leq \ \frac{4^c}{(x-1)^c}.$$

Then since $x > 16(c+1)(b+1)^c$, it must be true that $x > 5$, and thus

$$\frac{4^c}{(x-1)^c} \ < \ 1.$$

Then

$$0 \leq \ \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \ < \ 1,$$

so again our proposition holds.

Case 2: Let $b > 0$.
First, we will show that

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \ < \ b^c + 1.$$

Will will proceed by proving a series of inequalities.

(a.)

$$\boxed{\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \ \leq \ \frac{(bx+4)^c}{(x-1)^c}}$$

This inequality follows from Proposition 2.3.30, which tells us that

$$\alpha_{bx+4}(c+1) \leq (bx+4)^c$$

and

$$\alpha_x(c+1) \geq (x-1)^n.$$

.....

(b.)

$$\boxed{\frac{(bx+4)^c}{(x-1)^c} \leq \frac{\left(1+\frac{4}{x}\right)^c b^c}{\left(1-\frac{1}{x}\right)^c}}$$

Notice that

$$\frac{(bx+4)^c}{(x-1)^c} = \frac{\left(bx\left(1+\frac{4}{bx}\right)\right)^c}{\left(x\left(1-\frac{1}{x}\right)\right)^c} = \frac{b^c x^c \left(1+\frac{4}{bx}\right)^c}{x^c\left(1-\frac{1}{x}\right)^c} = \frac{b^c\left(1+\frac{4}{bx}\right)^c}{\left(1-\frac{1}{x}\right)^c}$$

Then since $\frac{4}{bx} \leq \frac{4}{x}$, it follows that

$$\frac{(bx+4)^c}{(x-1)^c} \leq \frac{\left(1+\frac{4}{x}\right)^c b^c}{\left(1-\frac{1}{x}\right)^c}$$

as desired.

.....

(c.)

$$\boxed{\frac{\left(1+\frac{4}{x}\right)^c b^c}{\left(1-\frac{1}{x}\right)^c} \leq \frac{b^c}{\left(1-\frac{1}{x}\right)^c\left(1-\frac{4}{x}\right)^c}}$$

Notice that

$$\frac{\left(1+\frac{4}{x}\right)^c b^c}{\left(1-\frac{1}{x}\right)^c} \leq \frac{b^c}{\left(1-\frac{1}{x}\right)^c\left(1-\frac{4}{x}\right)^c}$$

$$\iff \left(1+\frac{4}{x}\right)^c \leq \frac{1}{\left(1-\frac{4}{x}\right)^c}$$

$$\iff \left(1+\frac{4}{x}\right)^c \left(1-\frac{4}{x}\right)^c \leq 1 \text{ since } \left(1-\frac{4}{x}\right)^c > 0$$

$$\iff \left(\left(1+\frac{4}{x}\right)\left(1-\frac{4}{x}\right)\right)^c \leq 1$$

$$\iff \left(1-\frac{4}{x}+\frac{4}{x}-\frac{16}{x^2}\right)^c \leq 1$$

$$\iff \left(1-\frac{16}{x^2}\right)^c \leq 1.$$

Since $x \geq 16$, we know that

$$\frac{16}{x^2} < 1,$$

meaning

$$0 < \left(1-\frac{16}{x^2}\right) < 1$$

and so

$$\left(1-\frac{16}{x^2}\right)^c \leq 1.$$

Thus

$$\frac{\left(1+\frac{4}{x}\right)^c b^c}{\left(1-\frac{1}{x}\right)^c} \leq \frac{b^c}{\left(1-\frac{1}{x}\right)^c\left(1-\frac{4}{x}\right)^c}$$

as desired.

.....

(d.)

$$\boxed{\frac{b^c}{\left(1-\frac{1}{x}\right)^c\left(1-\frac{4}{x}\right)^c} \leq \frac{b^c}{\left(1-\frac{4}{x}\right)^{2c}}}$$

We know that

$$\frac{1}{x} < \frac{4}{x},$$

meaning

$$\left(1-\frac{1}{x}\right) > \left(1-\frac{4}{x}\right)$$

and therefore

$$\left(1-\frac{1}{x}\right)^c \geq \left(1-\frac{4}{x}\right)^c.$$

It then follows that

$$\frac{b^c}{\left(1-\frac{1}{x}\right)^c\left(1-\frac{4}{x}\right)^c} \leq \frac{b^c}{\left(1-\frac{4}{x}\right)^c\left(1-\frac{4}{x}\right)^c} = \frac{b^c}{\left(1-\frac{4}{x}\right)^{2c}}$$

as desired.

.....

(e.)

$$\boxed{\frac{b^c}{\left(1-\frac{4}{x}\right)^{2c}} \leq \frac{b^c}{1-\frac{8c}{x}}}$$

Here, we must show that

$$\left(1-\frac{4}{x}\right)^{2c} \geq 1-\frac{8c}{x}$$

for all c. This inequality will follow by induction.
Let c=0. Then

$$\left(1-\frac{4}{x}\right)^{2c} = 1 \geq 1 = 1-\frac{8c}{x}.$$

Then assume that for $c \leq k$,

$$\left(1 - \frac{4}{x}\right)^{2c} \geq 1 - \frac{8c}{x}.$$

Then let $c = k + 1$. Then

$$\begin{aligned}
\left(1 - \frac{4}{x}\right)^{2(k+1)} &= \left(1 - \frac{4}{x}\right)^{2k+2} \\
&= \left(1 - \frac{4}{x}\right)^{2k} \left(1 - \frac{4}{x}\right)^{2} \\
&\geq \left(1 - \frac{8k}{x}\right) \left(1 - \frac{4}{x}\right)^{2} \text{ by our induction hypothesis.} \\
&= 1 - \left(\frac{8 + 8k}{x}\right) + \left(\frac{16 + 64k}{x^2}\right) - \left(\frac{128k}{x^3}\right).
\end{aligned}$$

Notice that

$$\left(\frac{16 + 64k}{x^2}\right) - \left(\frac{128k}{x^3}\right) \geq 0$$

$$\iff 16x + 64xk - 128k \geq 0$$

$$\iff x + 4xk - 8k \geq 0$$

$$\iff x\,(1 + 4k) - 8k \geq 0.$$

Then by our initial assumption, we know that when $c = k+1$, $x \geq 16$, so in particular, $x \geq 8k$, and further $x \geq \frac{8k}{1+4k}$. Therefore

$$x\,(1 + 4k) - 8k \geq 0,$$

meaning

$$\left(\frac{16 + 64k}{x^2}\right) - \left(\frac{128k}{x^3}\right) \geq 0.$$

Then we get that

$$1 \; - \; \left(\frac{8+8k}{x}\right) \; + \; \left(\frac{16+64k}{x^2}\right) \; - \; \left(\frac{128k}{x^3}\right)$$

$$\geq \; 1 \; - \; \frac{8+8k}{x}$$

$$= \; 1 \; - \; \frac{8\,(k+1)}{x}.$$

Then when $c = k+1$, it holds that

$$\left(1-\frac{4}{x}\right)^{2c} \; \geq \; 1-\frac{8c}{x}.$$

Therefore, by induction, for all $c \geq 0$,

$$\left(1-\frac{4}{x}\right)^{2c} \; \geq \; 1-\frac{8c}{x}.$$

We can then conclude that

$$\frac{b^c}{\left(1-\frac{4}{x}\right)^{2c}} \; \leq \; \frac{b^c}{1-\frac{8c}{x}}$$

as desired.

.....

(f.)

$$\boxed{\frac{b^c}{1-\frac{8c}{x}} \; \leq \; b^c\left(1+\frac{16c}{x}\right)}$$

Notice that

$$\frac{b^c}{1-\frac{8c}{x}} \leq b^c\left(1+\frac{16c}{x}\right)$$

$$\iff \frac{1}{1-\frac{8c}{x}} \leq 1+\frac{16c}{x}$$

$$\iff \frac{x}{x-8c} \leq 1+\frac{16c}{x}$$

$$\iff \frac{x^2}{x-8c} \leq x+16c$$

$$\iff x^2 \leq (x+16c)(x-8c) \text{ since } x > 8c$$

$$\iff x^2 \leq x^2+8cx-128c^2$$

$$\iff 0 \leq 8cx-128c^2$$

$$\iff 0 \leq 8c(x-16c)$$

$$\iff c = 0 \text{ or } 0 \leq x-16c.$$

Then since $x > 16(c+1)(b+1)^c$, it must always be true that

$$0 < x-16c$$

and thus

$$\frac{b^c}{1-\frac{8c}{x}} \leq b^c\left(1+\frac{16c}{x}\right)$$

as desired.

.....

(g.)

$$\boxed{b^c\left(1+\frac{16c}{x}\right) \;<\; b^c+1}$$

Notice that

$$b^c\left(1+\frac{16c}{x}\right) \;<\; b^c+1$$

$$\iff b^c+\left(\frac{b^c 16c}{x}\right) \;<\; b^c+1$$

$$\iff \left(\frac{16cb^c}{x}\right) \;<\; 1$$

$$\iff 16cb^c \;<\; x.$$

Then since $x > 16(c+1)(b+1)^c$, it must be true that $x > 16cb^c$, and thus

$$b^c\left(1+\frac{16c}{x}\right) \;<\; b^c+1$$

as desired.

.....

Putting the seven previous inequalities together, we get that

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \;<\; b^c+1.$$

To prove our proposition, it remains to show that

$$b^c \;<\; \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)}.$$

This is easily done since, by Proposition 2.3.30, we know that

$$\alpha_{bx+4}(c+1) \;\geq\; (bx+3)^c$$

and

$$\alpha_x(c+1) \;\leq\; x^c,$$

meaning

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \;\geq\; \frac{(bx+3)^c}{x^c} \;=\; \left(\frac{bx+3}{x}\right)^c \;=\; (b+3x)^c \;\geq\; b^c.$$

Thus, combining Case 1 and Case 2, we can finally conclude that for all $b \geq 0$ and all $c \geq 0$, if $x > 16(c+1)(b+1)^c$, then

$$b^c \;\leq\; \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \;<\; b^c + 1.$$

□

Corollary 2.3.32. *If $x > 16(c+1)(b+1)^c$, then*

$$b^c = \alpha_{bx+4}(c+1) div \alpha_x(c+1).$$

Proof. By Proposition 2.3.31, we know that

$$b^c \;\leq\; \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \;<\; b^c + 1.$$

for $x > 16(c+1)(b+1)^c$. Then the integer part of $\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)}$ must be b^c. □

Recall that in Example 2.3.32, we found that the *div* function is diophantine. Therefore, Corollary 2.3.32 provides us with the desired diophantine way of expressing b^c in terms of α_b. The only slight problem left to deal with is expressing the condition $x > 16(c+1)(b+1)^c$ in a Diophantine way. We solve this problem easily with the following theorem.

Proposition 2.3.33. *If $x = 16(c+1)\alpha_{b+4}(c+1)$, then $x > 16(c+1)(b+1)^c$.*

Proof. Using Proposition 2.3.30, we get that

$$\alpha_{b+4}(c+1) \;\geq\; (b+3)^c \;\geq\; (b+1)^c.$$

□

Note that there are obviously an infinite number of choices of x that would fulfill the requirement that $x > 16(c+1)(b+1)^c$. The reason for using α_{b+4} is simply that

is automatically fulfills the condition that the base of α be greater than or equal to 4.

We have now seen that we can represent the set

$$\{\langle a, b, c\rangle \mid a = b^c\}$$

by the set

$$\{\langle a, b, c\rangle \mid x = 16(c+1)\alpha_{b+4}(c+1) \text{ and } a = \alpha_{bx+4}(c+1)div\alpha_x(c+1)\}.$$

In order to make the conditions

$$x = 16(c+1)\alpha_{b+4}(c+1) \text{ and } a = \alpha_{bx+4}(c+1)div\alpha_x(c+1)$$

Diophantine, we can replace α_{b+4}, α_{bx+4}, and $\alpha_x(c+1)$ each with the set of conditions given in Proposition 2.3.27. Thus, the set $\{\langle a, b, c\rangle \mid a = b^c\}$ is Diophantine.

Part III

Background: Computability Theory

Chapter 3

Key Concepts and Definitions

3.1 Register Machines

In order to understand Hilbert's tenth problem, we first needed to understand Diophantine equations and Diophantine sets. In addition, we need to specify what is meant by "devis[ing] a process" that determines if Diophantine equations have solutions. In modern times, this "process" can be thought of as an algorithm, so the question of whether or not a Diophantine equation has solutions can be thought of as a question of computability. Thus, we now turn to giving a background on the computability concepts necessary in understanding Hilbert's tenth problem and its negative solution. In this section, we will examine a model of computation known as a register machine.

Definition 3.1.1. A *register machine* M consists of a finite number of registers R_1, ..., R_n, each of which can hold a natural number, and a finite length program of instructions $L_0, ..., L_m$, where each instruction L_i must have one of the following forms:

- L_i: $R_k \to R_k + 1$ (and GO TO L_{i+1})

- L_i: If $R_k \neq 0$, then $R_k \to R_k - 1$ and GO TO L_j
  If $R_k = 0$, then GO TO L_{i+1}

- L_i: HALT

In order to understand this definition better, let's look at some examples. Our first example is a machine that can be used to add two natural numbers together.

Example 3.1.2. Let M consist of two registers R_1 and R_2 and the following program:

- L_0: $R_1 \to R_1 + 1$ (and GO TO L_1)
- L_1: If $R_2 \neq 0$, then $R_2 \to R_2 - 1$ and GO TO L_0 (else GO TO L_2)
- L_2: If $R_1 \neq 0$, then $R_1 \to R_1 - 1$ and GO TO L_3 (else GO TO L_3)
- L_3: HALT

Then suppose the initial input in R_1 is 2 and the initial input in R_2 is 3. Then the following diagram represents the progression of M:

R_1 :	2	3	3	4	4	5	5	6	6	5
R_2 :	3	3	2	2	1	1	0	0	0	0
Next Instruction:	L_0	L_1	L_0	L_1	L_0	L_1	L_0	L_1	L_2	L_3

Instead, suppose the initial input in R_1 is 13 and the initial input in R_2 is 4. Then the following diagram represents the progression of M:

R_1 :	13	14	14	15	15	16	16	17	17	18	18	17
R_2 :	4	4	3	3	2	2	1	1	0	0	0	0
Next Instruction:	L_0	L_1	L_0	L_1	L_0	L_1	L_0	L_1	L_0	L_1	L_2	L_3

For a third case, suppose the initial input in R_1 is 5 and the initial input in R_2 is 0. Then the following diagram represents the progression of M:

R_1 :	5	6	6	5
R_2 :	0	0	0	0
Next Instruction:	L_0	L_1	L_2	L_3

Note that the progression of the register machine M is different for different initial inputs. In particular, the order of the insturctions used, the contents of R_1 and R_2 at each step, and the number of steps used before reaching the halt instruction, all vary depending on the initial input.

It is also possible that, on some or all inputs, a register machines will never reach the halt instruction, as shown in the following example.

Example 3.1.3. Let M consist of one register R_1 and the following program:

- L_0: $R_1 \to R_1 + 1$
- L_1: If $R_1 \neq 0$ then $R_1 \to R_1 - 1$ and GO TO L_0
- L_2: HALT

Then let the initial input of R_1 be some natural number n. Then the following diagram represents the progression of M:

R_1 :	n	$n+1$	n	$n+1$	n	...
Next Instruction:	L_0	L_1	L_0	L_1	L_0	...

Thus, on any input, this register machine enters an infinite loop and never reaches HALT.

3.2 Computable and Computably Enumberable Sets

Now that we know the definition of a register machine, we can define a computably enumerable set.

Definition 3.2.1. A set S of n-tuples is called *computably enumerable* when there exists a register machine M such that M reaches a halt on input $a_1, ..., a_n$ if and only if $\langle a_1, ..., a_n \rangle \in S$.

Note that this definition requires that M runs forever on any input that is not in S. However, as a register machine progresses on some input, we may not be able to tell if the machine will run forever, or if it simply has not reached a halt yet. Thus, a stronger classification of sets is the computable set, defined as follows:

Definition 3.2.2. A set S of n-tuples is called $RM-computable$ when there exists a register machine M such that on input $a_1, ..., a_n$, M halts with output 1 if and only if $\langle a_1, ..., a_n \rangle \in S$ and with output 0 if and only if $\langle a_1, ..., a_n \rangle \notin S$.

Thus, if a set is computable, we have a definitive way of checking whether any given n-tuple is in the set. To show that Hilbert's problem is unsolvable, we will show that Diophantine sets are not computable, which implies that we have no way of checking whether or not the Diophantine equation that represents the set has natural number solutions (if there was a way, then the set would be computable). In order to do this, we will make use of the following well-known theorem.

Theorem 3.2.3. *A set S is computable if and only if S and S^c are computably enumerable.*

Now that we have a background on Diophantine sets and the appropriate computability concepts, we are prepared to prove the unsolvability of Hilbert's Tenth Problem. We will begin with a comparison of Diophantine and computably enumerable sets.

Part IV

The Proof

Chapter 4

Comparison of Diophantine and C.E. Sets

In this chapter, we will see that a set is Diophantine if and only if it is computably enumerable. In general, it is a trivial fact that any Diophantine set is computably enumerable. If a set is Diphantine, then we know that there is some Diophantine equation that represents the set. Therefore, we can build a register machine, based on this equation, which will halt if and only if an input is a solution, making the set computably enumerable. On the other hand, it is not so obvious that a computably enumerable set is Diophantine. Our goal in the following sections will be to prove that it is.

4.1 Further Examination of Register Machines

By definition, we know that if a set S is computably enumerable, then there is a register machine M such that on input x, M reaches a halt if and only if $x \in S$. We also know that M must have some finite number of registers, call them R_1, R_2, ...,R_n, and some finite number of instructions, call them L_0, L_1, ..., L_m. To picture M_x, the progression of M on some input $x \in S$, we can use the following diagram:

	t=0	t=1	t=2	...	t=s
R_1	$r_{1,0} = x$	$r_{1,1}$	$r_{1,2}$	...	$r_{1,s}$
R_2	$r_{2,0} = 0$	$r_{2,1}$	$r_{2,2}$	...	$r_{2,s}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
R_n	$r_{n,0} = 0$	$r_{n,1}$	$r_{n,2}$	...	$r_{n,s}$
L_0	$l_{0,0} = 1$	$l_{0,1}$	$l_{0,2}$	...	$l_{0,s}$
L_1	$l_{1,0} = 0$	$l_{1,1}$	$l_{1,2}$	...	$l_{1,s}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
L_m	$l_{m,0} = 0$	$l_{m,1}$	$l_{m,2}$	...	$l_{m,s}$

where

- s is the number of steps that it takes for M to reach a halt on input $x \in S$
- each $r_{i,t}$ is the entry in register R_i at time t
- and each
$$l_{i,t} = \begin{cases} 1, & \text{if } L_j \text{ is the next instruction at time } t \\ 0, & \text{else.} \end{cases}$$

In order for M_x to be a valid progression of M, the values of each $r_{i,t}$ and each $l_{j,t}$ must fit a number of characteristics, including the following:

- The first instruction must be L_0,
i.e. $l_{0,0} = 1$.
- At any particular time t, there must be exactly one instruction that comes next, i.e. for any t, there exists some $j \in [0, m]$ such that $l_{j,t} = 1$ and for all $k \in [0, m]$, $k \neq i$, $l_{k,t} = 0$.
- The only halt instruction is the last instruction,
i.e. $l_{m,s} = 1$, where L_m is the halt instruction, and for all $t \neq s$, $l_{m,t} = 0$.
- At any time t, the values of $r_{1,t}$, ..., $r_{n,t}$ and $l_{0,t}$, ..., $l_{m,t}$ result from applying one of the possible RM instructions, as described in Definition 3.1.1, to the values of $r_{1,t-1}$,...,$r_{n,t-1}$ and $l_{0,t-1}$,...,$l_{m,t-1}$.

Note that for any $x \in S$, the values of each $r_{i,t}$ and each $l_{j,t}$ will have these properties, and if there are values of each $r_{i,t}$ and each $l_{j,t}$ that have these properties for some x, then $x \in S$. Therefore, to show that S is Diophantine, we will rewrite the above conditons as Diophantine conditions that hold if and only if $x \in S$.

4.2 Preparation for Determining Diophantine Conditions

In order to determine the system of Diophantine conditions that are met if and only if $x \in S$, we must first determine what constants, parameters, and variables we will need. Since we have a particular register machine M associated with our set S, the values of m and n are constants. Our parameter will be x, representing any input we might put into M. Since the number of steps in M_x varies with each input x, s will be a variable. We might also attempt to make each value of $r_{i,t}$ and $l_{j,t}$ variables as well, but since s changes with each step, each input x would require a different number of variables. Instead, note that we could take our register machine and define the values R_1^*, ..., R_n^*, L_0^*, ..., L_m^*, where

- for any $i \in [1, n]$, $R_i^* = \sum_{t=0}^{s} r_{i,t} \cdot Q^t$ for some $Q \in \mathbb{N}$
- for any $j \in [0, m]$, $L_j^* = \sum_{t=0}^{s} l_{j,t} \cdot Q^t$ for some $Q \in \mathbb{N}$.

Note that as long as Q is a large enough base, each $r_{i,t}$ and each $l_{j,t}$ could be uniquely recovered from each R_i^* and each L_j^*. With this value of Q, we could also define the value I, where

- $I = \sum_{t=0}^{s} 1 \cdot Q^t$.

So, the variables in our Diophantine conditions will include s, Q, I, R_1^*, ..., R_n^*, and L_0^*, ..., L_m^*.

In addition, we will also make use of a new binary relation, $\preceq$.

Definition 4.2.1. Let r and s be two numbers written in base 2 notation, i.e.

$$r = \sum_{i=0}^{y} r_i 2^i \ (0 \leq r_i \leq 1) \ \ \textit{and} \ \ s = \sum_{i=0}^{y} s_i 2^i \ (0 \leq s_i \leq 1)$$

for some $y \in \mathbb{N}$. Then $r \preceq s$ if and only if $r_i \leq s_i$ for all $i \in [0, y]$.

In order to show that $\preceq$ is a Diophantine relation, we will use the following lemma, without proof.

Lemma 4.2.2. *$r \preceq s$ if and only if $\binom{s}{r} = 1 \bmod 2$.*

Theorem 4.2.3. *$\preceq$ is a Diophantine relation.*

Proof. In Example 2.2.2, we saw that the choose function is Diophantine, and in Example 2.1.4, we saw that the congruence relation is Diophantine. Therefore, by Lemma 4.2.2, $\preceq$ is a Diophantine relation. □

With these preparations in place, we can now determine the Diophantine conditions that represent S.

4.3 Determining the Diophantine Conditions

We will proceed by examining each desired characteristic individually and the appropriate Diophantine condition(s) that can be used to represent them.

.....

Property: Q must be a sufficiently large base to uniquely determine each $r_{i,t}$ and each $l_{j,t}$.

Diophantine Conditions: $x + s < \frac{Q}{2}$ and $m + 1 < Q$.

Reasoning: At any time t, $r_{i,t}$ cannot be any larger than $x + t$. Thus, any $Q > x + s$ would suffice to uniquely determine each $r_{i,t}$. We instead require that $Q > 2(x + s)$ for later reasons. Further, since each $l_{j,t}$ is no larger than 1, $Q > 1$ is sufficiently large. We instead require that $Q > m + 1$ for later reasons.

.....

Note that our intention is to set condtions on the values of each $r_{i,t}$ and $l_{j,t}$, and the above property allows us to do so by setting conditions on the values of R_1^*, ..., R_n^*, L_0^*, ..., L_m^* when examined base Q. However, the Diophantine relation that we have at our disposal is $\preceq$, which compares values base 2 rather than base Q. Therefore, we will set the following condition on Q to make it easier for us to convert back and forth between values written in base 2 and base Q.

.....

Property: Q is some power of 2.

Diophantine Condition: $Q \preceq 2Q - 1$

Reasoning: Take any value $Q \in \mathbb{N}$. Then the values Q, $2Q$, and $2Q - 1$ can be written in base 2 as

		...	$\times 2^{k+1}$	$\times 2^k$	...	$\times 2^1$	$\times 2^0$
Q	=	...	a_{k+1}	a_k	...	a_1	a_0
$2Q$	=	...	a_k	a_{k-1}	...	a_0	0
1	=	0	0	0	0	0	1

where each $0 \leq a_i \leq 1$. Also, note that Q is a power of 2 if and only if there is a unique i such that $a_i = 1$.

Since we know that $Q > 1$, we know that there is at least one i such that $a_i = 1$. Then let k be the lowest value of i such that $a_i = 1$. Then in subtracting 1 from $2Q$, we obtain the following:

			...	$\times 2^{k+1}$	$\times 2^k$	...	$\times 2^1$	$\times 2^0$
	Q	=	...	a_{k+1}	1	0	0	0
	$2Q$	=	...	1	0	0	0	0
$-$	1	=	0	0	0	0	0	1
	$2Q - 1$	=	...	0	1	1	1	1

Note that for all values of i that are visible in the above chart, the condition $Q \preceq 2Q - 1$ holds. Now suppose that there is some $h > k$ such that $a_h = 1$ as well. If $h = k + 1$, i.e. if $a_{k+1} = 1$, we can see from the above diagram that our condition $Q \preceq 2Q - 1$ is no longer satisfied, as the coefficient on 2^{k+1} in Q would be 1, while the coefficient on 2^{k+1} in $2Q - 1$ would be 0. Thus, we can assume that $a_{h-1} = 0$, meaning that after subtraction, the coefficient on 2^h in $2Q - 1$ is 0. Again, this contradicts our condition, as we assumed that the coefficient on 2^h in Q is 1. This contradiction can be illustrated as follows:

			...	$\times 2^h$	$\times 2^{h-1}$	...	$\times 2^{k+1}$	$\times 2^k$	...	$\times 2^1$	$\times 2^0$
	Q	=	...	1	0	...	0	1	0	0	0
	$2Q$	=	...	0	...	...	1	0	0	0	0
$-$											
	1	=	0	0	0	0	0	0	0	0	1
	$2Q-1$	=	...	0	...	...	0	1	1	1	1

Therefore, the condition $Q \preceq 2Q-1$ guarantees that there is only one value of i such that $a_i = 1$, and thus that Q is a power of 2.

.....

Property: An arbitraty $I \in \mathbb{N}$ has the form $I = \sum_{t=0}^{s} Q^t$

Diophantine Condition: $1 + (Q-1)I = Q^{s+1}$

Reasoning: Using the formula for a geometric series, we get that

$$I = \frac{Q^{s+1}-1}{Q-1}.$$

.....

For the remaining properties, it will be useful to examine the conversion between a number written in base Q and that number written in base 2. Let $N \in \mathbb{N}$. First, let's examine N in base Q. We know that we can write any N as

$$N = \sum_t q_t \cdot Q^t \text{ where } 0 \leq q_t < Q.$$

Then since Q is some k-th power of 2, we can write N out in base Q as follows:

	...	$\times Q^2$	$\times Q^1$	$\times Q^0$		...	$\times (2^k)^2$	$\times (2^k)^1$	$\times (2^k)^0$
$N =$	...	q_2	q_1	q_0	=	...	q_2	q_1	q_0

Next, let's examine N in base 2. We know that we can write N as

$$N = \sum_v u_v \cdot 2^v \text{ where } 0 \leq u_v \leq 1.$$

Then N written in base 2 will be as follows:

	...	$\times 2^{2k}$	$\times 2^{2k-1}$	...	$\times 2^{k+1}$	$\times 2^k$	$\times 2^{k-1}$	...	$\times 2^1$	$\times 2^0$
$N =$	...	u_{2k}	u_{2k-1}	...	u_{k+1}	u_k	u_{k-1}	...	u_1	u_0

Now, suppose we want to convert between N written in base Q and N written in base 2. For a particular t, we know that the value of q_t can range from 0 to $2^{k-1}+1$. Then let's consider the value of $q_t \cdot Q^t$ for the various possibilities of q_t.

q_t	$q_t \cdot Q^t$	value $q_t \cdot Q^t$ written in base 2						
		...	$\times 2^{kt+(k-1)}$	...	$\times 2^{kt+2}$	$\times 2^{kt+1}$	$\times 2^{kt}$	...
0	$(0) \cdot 2^{kt}$	0	0	0	0	0	0	0
1	$(2^0) \cdot 2^{kt}$	0	0	0	0	0	1	0
2	$(2^1) \cdot 2^{kt}$	0	0	0	0	1	0	0
3	$(2^1 + 2^0) \cdot 2^{kt}$	0	0	0	0	1	1	0
4	$(2^2) \cdot 2^{kt}$	0	0	0	1	0	0	0
5	$(2^2 + 2^0) \cdot 2^{kt}$	0	0	0	1	0	1	0
6	$(2^2 + 2^1) \cdot 2^{kt}$	0	0	0	1	1	0	0
7	$(2^2 + 2^1 + 2^0) \cdot 2^{kt}$	0	0	0	1	1	1	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^{k-1}	$(2^{k-1}) \cdot 2^{kt}$	0	1	0	0	0	0	0
$2^{k-1}+1$	$(2^{k-1} + 2^0) \cdot 2^{kt}$	0	1	0	0	0	1	0

The important thing to notice here is that for any t, the value $q_t \cdot Q^t$ written in base 2 only ever has a 1 as the coefficients on 2^{kt} through $2^{kt+(k-1)}$. Therefore, each q_t determines exactly the values of u_{kt} through $u_{kt+(k-1)}$. For example, q_0 determines u_0 through u_{k-1}, q_1 determines u_k through u_{2k-1}, q_2 determines u_{2k} through u_{3k-1}, and so on. In particular, for any t,

$$u_{kt+(k-1)} \ldots u_{kt+1} u_{kt}$$

is the value of q_t written out in base 2. Now that we understand this relationship, we can continue examining the remaining properties.

.....

Property: An arbitrary $R_i^* \in \mathbb{N}$ has the form $R_i^* = \sum_{t=0}^{s} r_{i,t} \cdot Q^t$ $(0 \leq r_{i,t} \leq \frac{Q}{2})$

Diophantine Condition: $R_i^* \preceq (\frac{Q}{2} - 1)I$ for all $i = 1, 2, ..., n$

Reasoning: We know that we can write any arbitrary $R_i^* \in \mathbb{N}$ as $R_i^* = \sum_{t} r_{i,t} \cdot Q^t$ with $0 \leq r_{i,t} < Q$ for all t. Therefore, we just need to show that the condition $R_i^* \preceq (\frac{Q}{2} - 1)I$ guarantees that s is a large enough bound for this summation, i.e. that for all $t > s$, $r_{i,t} = 0$, and that for all $t \in [0, s]$, $r_{i,t} < \frac{Q}{2}$. Since we know that Q is some k-th power of 2 and $I = \sum_{t=0}^{s} Q^t$, we find that

$$\left(\frac{Q}{2} - 1\right) I = \sum_{t=0}^{s} \left(2^{k-1} - 1\right) \cdot Q^t.$$

Then since $2^{k-1} - 1 < Q$, so the coefficients on Q^0 through Q^s when $(\frac{Q}{2} - 1)I$ is written in base Q will be $2^{k-1} - 1$. Also, note that the value $2^{k-1} - 1$ written in base 2 can be determined as follows:

			$\times 2^{k-1}$	...	$\times 2^1$	$\times 2^0$
	2^{k-1}	=	1	0	0	0
$-$						
	1	=	0	0	0	1
	$2^{k-1} - 1$	=	0	1	1	1

Therefore, by our previous examination of converting between base Q and base 2, we know that we can write $\left(\frac{Q}{2} - 1\right) I$ in base 2 as

$$= \begin{array}{cccccccccccccccccccc} & +2^{(s+2)k-1} & & \dots & & +2^{(s+1)k+1} & & +2^{(s+1)k} & & +2^{(s+1)k-1} & & \dots & & +2^{sk+1} & & +2^{sk} & \dots & +2^{2k-1} & & \dots & & +2^{k+1} & & +2^{k} & & +2^{k-1} & & \dots & & +2^{1} & & +2^{0} \\ & \boxed{0} & & \boxed{0} & & \boxed{0} & & \boxed{0} & & \boxed{0} & & \boxed{1} & & \boxed{1} & & \boxed{1} & \dots & \boxed{0} & & \boxed{1} & & \boxed{1} & & \boxed{1} & & \boxed{0} & & \boxed{1} & & \boxed{1} & & \boxed{1} \end{array}$$

Then by the condition $R_i^* \preceq (\frac{Q}{2} - 1)I$, R_i^* written in base 2 and Q notation is

$$= \begin{array}{cccccccccccccccccccc} & +2^{(s+2)k-1} & & \dots & & +2^{(s+1)k+1} & & +2^{(s+1)k} & & +2^{(s+1)k-1} & & \dots & & +2^{sk+1} & & +2^{sk} & \dots & +2^{2k-1} & & \dots & & +2^{k+1} & & +2^{k} & & +2^{k-1} & & \dots & & +2^{1} & & +2^{0} \\ & \boxed{0} & & \boxed{0} & & \boxed{0} & & \boxed{0} & & \boxed{0} & & \boxed{?} & & \boxed{?} & & \boxed{?} & \dots & \boxed{0} & & \boxed{?} & & \boxed{?} & & \boxed{?} & & \boxed{0} & & \boxed{?} & & \boxed{?} & & \boxed{?} \end{array}$$

$$= \begin{array}{cccccccc} & \times Q^{s+1} & & & \times Q^{s} & & \dots & \times Q^{1} & & & \times Q^{0} \\ & \boxed{0} & & & \boxed{r_{i,s}} & & & \boxed{r_{i,1}} & & & \boxed{r_{i,0}} \end{array}$$

Therefore, for all $t > s$, $r_{i,t} = 0$, and for all $t \in [0, s]$, $r_{i,t} < \frac{Q}{2}$ (if it weren't, then the coefficient on each 2^{tk-1} in R_i^* would not be a 0). Thus, our condition guarantees that $R_i^* \in \mathbb{N}$ has the desired form.

.....

Property: An arbitrary $L_j^* \in \mathbb{N}$ has the form $L_j^* = \sum_{t=0}^{s} l_{j,t} \cdot Q^t$ $(0 \leq l_{j,t} \leq 1)$.

Diophantine Condition: $L_j^* \preceq I$ for all $j = 0, 1, ..., m$

Reasoning: Again, any $L_{j,t}^* \in \mathbb{N}$ can be written as $\sum_{t=0} l_{j,t} \cdot Q^t$ $(0 \leq l_{j,t} < Q)$. Therefore, we just need to show that our condition guarantees that s is a large enough bound for this summation, i.e. that for all $t > s$, $l_{j,t} = 0$, and that for all $t \in [0, s]$, $0 \leq l_{j,t} \leq 1$. First, note that I in base 2 and base Q is

$$= \overset{\times Q^{s+1}}{\boxed{0}} \qquad \overset{\times Q^{s}}{\boxed{1}} \qquad ... \qquad \overset{\times Q^{1}}{\boxed{1}} \qquad \overset{\times Q^{0}}{\boxed{1}}$$

$$= \overset{+2^{(s+2)k-1}}{\boxed{0}} \overset{...}{\boxed{0}} \overset{+2^{(s+1)k+1}}{\boxed{0}} \overset{+2^{(s+1)k}}{\boxed{0}} \quad \overset{+2^{(s+1)k-1}}{\boxed{0}} \overset{...}{\boxed{0}} \overset{+2^{sk+1}}{\boxed{0}} \overset{+2^{sk}}{\boxed{1}} \quad ... \quad \overset{+2^{2k-1}}{\boxed{0}} \overset{...}{\boxed{0}} \overset{+2^{k+1}}{\boxed{0}} \overset{+2^{k}}{\boxed{1}} \quad \overset{+2^{k-1}}{\boxed{0}} \overset{...}{\boxed{0}} \overset{+2^{1}}{\boxed{0}} \overset{+2^{0}}{\boxed{1}}$$

Then by the condition $L_j^* \preceq I$, we find that L_j^* in base 2 and base Q is

$$= \overset{+2^{(s+2)k-1}}{\boxed{0}} \overset{...}{\boxed{0}} \overset{+2^{(s+1)k+1}}{\boxed{0}} \overset{+2^{(s+1)k}}{\boxed{0}} \quad \overset{+2^{(s+1)k-1}}{\boxed{0}} \overset{...}{\boxed{0}} \overset{+2^{sk+1}}{\boxed{0}} \overset{+2^{sk}}{\boxed{?}} \quad ... \quad \overset{+2^{2k-1}}{\boxed{0}} \overset{...}{\boxed{0}} \overset{+2^{k+1}}{\boxed{0}} \overset{+2^{k}}{\boxed{?}} \quad \overset{+2^{k-1}}{\boxed{0}} \overset{...}{\boxed{0}} \overset{+2^{1}}{\boxed{0}} \overset{+2^{0}}{\boxed{?}}$$

$$= \overset{\times Q^{s+1}}{\boxed{0}} \qquad \overset{\times Q^{s}}{\boxed{1 \text{ or } 0}} \qquad ... \qquad \overset{\times Q^{1}}{\boxed{1 \text{ or } 0}} \qquad \overset{\times Q^{0}}{\boxed{1 \text{ or } 0}}$$

Therefore, the condition $L_j^* \preceq I$ guarantees that L_j^* has the desired form.

.....

Property: For any $t \in [0, s]$, there is exactly one $j \in [0, m]$ such that $l_{j,t} = 1$.

Diophantine Condition: $I = \sum_{j=0}^{m} L_j^*$ (Note that this is a Diophantine condition because m is a constant.)

Reasoning: As we just examined, the condition $L_j^* \preceq I$ for $j = 0, 1, ..., m$ guarantees that for $j = 0, 1, ..., m$, L_j^* in base 2 is

		$+2^{(s+1)k-1}$	...	$+2^{sk+1}$	$+2^{sk}$		$+2^{2k-1}$	...	$+2^{k+1}$	$+2^{k}$	$+2^{k-1}$	...	$+2^{1}$	$+2^{0}$
L_j^*	=	0	0	0	?	...	0	0	0	?	0	0	0	?

Then the condition $I = \sum_{j=0}^{m} L_j^*$ guarantees that

		$+2^{(s+1)k-1}$	...	$+2^{sk+1}$	$+2^{sk}$		$+2^{2k-1}$	...	$+2^{k+1}$	$+2^{k}$	$+2^{k-1}$	...	$+2^{1}$	$+2^{0}$
L_1^*	=	0	0	0	?	...	0	0	0	?	0	0	0	?
+														
L_2^*	=	0	0	0	?	...	0	0	0	?	0	0	0	?
+														
$\vdots$				$\vdots$					$\vdots$				$\vdots$	
+														
L_m^*	=	0	0	0	?	...	0	0	0	?	0	0	0	?
I	=	0	0	0	1	...	0	0	0	1	0	0	0	1

Note that each of the columns of the coefficients on 2^0, 2^k, 2^{2k}, ..., 2^{sk} (we will refer to these as the columns of interest) has $k-1$ columns of all zeroes to its left. Also, note that at most, any column of interest could have $m+1$ 1's. If this were the case, then during addition we would carry a value of $\frac{m+1}{2}$ or $\frac{m}{2}$ (whichever is an integer) over to the next column to the left. If this value were large enough, then we would end up carrying a value of $\frac{m+1}{2^2}$ or $\frac{m}{2^2}$ over to the next column to the left, and so on. Our concern would be that this value eventually gets carried all the way to the next column of interest. In order for this to happen, either $\frac{m+1}{2^k} > 1$, or $\frac{m}{2^k} > 1$. However, recall that in our first condition, we set $Q = 2^k > m+1$. Therefore, the possibility of any value getting carried into a column of interest during addition is eliminated. Thus, for any column of interest,

- if there are no 1's, the value of I in this column will be a 0, a contradiction to our condition.

- if there is a single 1, the value of I in this column is a 1, as required by our condition.
- if the number of 1's is greater than 1 and even, the value of I in this column will be a 0, a contradiction to our condition.
- if the number of 1's is greater than 1 and odd, then the value of I in some column to the left (but before the next column of interest) will be a 1, a contradiction to our condition.

Thus, the condition $I = \sum_{j=0}^{m} L_j^*$ guarantees that for any $t \in [0, s]$, there is exactly one $j \in [0, m]$ such that $l_{j,t} = 1$.

.....

Property: $l_{0,0} = 1$.

Diophantine Condition: $1 \preceq L_0^*$

Reasoning: We know that 1 in base 2 is

	$+2^{(s+1)k-1}$	...	$+2^{sk+1}$	$+2^{sk}$	...	$+2^{2k-1}$	...	$+2^{k+1}$	$+2^k$	$+2^{k-1}$	...	$+2^1$	$+2^0$
$1 =$	0	0	0	0	...	0	0	0	0	0	0	0	1

Then the condition $1 \preceq L_0^*$ guarantees that L_0^* in base 2 must be

	$+2^{(s+1)k-1}$	...	$+2^{sk+1}$	$+2^{sk}$	...	$+2^{2k-1}$	...	$+2^{k+1}$	$+2^k$	$+2^{k-1}$	...	$+2^1$	$+2^0$
$L_0^* =$	?	?	?	?	...	?	?	?	?	?	?	?	1

Thus, $l_{0,0} = 1$, as desired.

.....

Property: $l_{m,t} = 1$ if and only if $t = s$, where L_m is the halt instruction.

Diophantine Condition: $L_m^* = Q^s$

Reasoning: The condition $L_m^* = Q^s$ implies that L_m^* in base Q is

		$\times Q^s$	$\times Q^{s-1}$		$\times Q^1$	$\times Q^0$
L_m^*	=	1	0	...	0	0

Thus $l_{m,s} = 1$ and for all $t \neq s$, $l_{m,t} = 0$, as desired.

.....

The conditions that follow can be used to ensure the property that at any time t, the values of $r_{1,t}$, ..., $r_{n,t}$, $l_{0,t}$, ..., $l_{m,t}$ are determined by applying the appropriate instruction of M to the values $r_{1,t-1}$, ..., $r_{n,t-1}$, $l_{0,t-1}$, ..., $l_{m,t-1}$. Thus, these conditions will depend on the particular instructions L_0, ..., L_m that make up M.

.....

For any $j \in [0, m]$ such that the instruction L_j is GO TO L_p, we include a copy of the following condition.

Diophantine Condition: $QL_j^* \preceq L_p^*$

Reasoning: In base Q, we know that L_j^* is

		$\times Q^s$	$\times Q^{s-1}$		$\times Q^1$	$\times Q^0$
L_j^*	=	0	$l_{j,s}$	...	$l_{j,1}$	$l_{j,0}$

Then QL_j^* in base Q and base 2 is

$$= \boxed{l_{j,s}}^{\times Q^{s+1}} \quad \boxed{l_{j,s-1}}^{\times Q^{s}} \quad \ldots \quad \boxed{l_{j,0}}^{\times Q^{1}} \quad \boxed{0}^{\times Q^{0}}$$

$$= \boxed{0}^{+2^{(s+2)k-1}} \ldots \boxed{0}^{+2^{(s+1)k+1}} \boxed{0}^{+2^{(s+1)k}} \boxed{l_{j,s}} \quad \boxed{0}^{+2^{(s+1)k-1}} \ldots \boxed{0}^{+2^{sk+1}} \boxed{0}^{+2^{sk}} \boxed{l_{j,s-1}} \quad \ldots \quad \boxed{0}^{+2^{2k-1}} \boxed{0}^{+2^{k+1}} \boxed{0}^{+2^{k}} \boxed{l_{j,0}} \quad \boxed{0}^{+2^{k-1}} \ldots \boxed{0}^{+2^{1}} \boxed{0}^{+2^{0}}$$

Further, L_p^* in base Q and base 2 is

$$= \boxed{0}^{\times Q^{s+1}} \quad \boxed{l_{p,s}}^{\times Q^{s}} \quad \ldots \quad \boxed{l_{p,1}}^{\times Q^{1}} \quad \boxed{l_{p,0}}^{\times Q^{0}}$$

$$= \boxed{0}^{+2^{(s+2)k-1}} \ldots \boxed{0}^{+2^{(s+1)k+1}} \boxed{0}^{+2^{(s+1)k}} \boxed{0} \quad \boxed{0}^{+2^{(s+1)k-1}} \ldots \boxed{0}^{+2^{sk+1}} \boxed{0}^{+2^{sk}} \boxed{l_{p,s}} \quad \ldots \quad \boxed{0}^{+2^{2k-1}} \boxed{0}^{+2^{k+1}} \boxed{0}^{+2^{k}} \boxed{l_{p,1}} \quad \boxed{0}^{+2^{k-1}} \ldots \boxed{0}^{+2^{1}} \boxed{l_{p,0}}^{+2^{0}}$$

Thus, for any t, the value $l_{j,t}$ is compared with the value $l_{p,t+1}$. Therefore, the condition $QL_j^* \preceq L_p^*$ guarantees that for any t, if $l_{j,t} = 1$, then $l_{p,t+1} = 1$.

.....

For any $j \in [0, m]$ such that the instruction L_j is IF $R_i = 0$, GO TO L_p (IF $R_i \neq 0$, GO TO L_{j+1}), we include a copy of the following conditions.

Diophantine Conditions: $QL_j^* \preceq L_p^* + L_{j+1}^*$ and $QL_j^* \preceq L_{j+1}^* + QI - 2R_j^*$

Reasoning:

First, we will show that the condition $QL_j^* \preceq L_p^* + L_{j+1}^*$ guarantees that for any t such that $l_{j,t} = 1$, either $l_{j,t+1} = 1$ or $l_{p,t+1} = 1$. We know that QL_j^*in base Q and base 2 is

$$= \quad \overset{\times Q^{s+1}}{\boxed{l_{j,s}}} \qquad \overset{\times Q^{s}}{\boxed{l_{j,s-1}}} \qquad \ldots \qquad \overset{\times Q^{1}}{\boxed{l_{j,0}}} \qquad \overset{\times Q^{0}}{\boxed{0}}$$

$$= \quad \overset{+2^{(s+2)k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{(s+1)k+1}}{\boxed{0}} \; \overset{+2^{(s+1)k}}{\boxed{l_{j,s}}} \qquad \overset{+2^{(s+1)k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{sk+1}}{\boxed{0}} \; \overset{+2^{sk}}{\boxed{l_{j,s-1}}} \qquad \ldots \qquad \overset{+2^{2k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{k+1}}{\boxed{0}} \; \overset{+2^{k}}{\boxed{l_{j,0}}} \qquad \overset{+2^{k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{1}}{\boxed{0}} \; \overset{+2^{0}}{\boxed{0}}$$

Further, L_p^* in base Q and base 2 is

$$= \quad \overset{\times Q^{s+1}}{\boxed{0}} \qquad \overset{\times Q^{s}}{\boxed{l_{p,s}}} \qquad \ldots \qquad \overset{\times Q^{1}}{\boxed{l_{p,1}}} \qquad \overset{\times Q^{0}}{\boxed{l_{p,0}}}$$

$$= \quad \overset{+2^{(s+2)k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{(s+1)k+1}}{\boxed{0}} \; \overset{+2^{(s+1)k}}{\boxed{0}} \qquad \overset{+2^{(s+1)k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{sk+1}}{\boxed{0}} \; \overset{+2^{sk}}{\boxed{l_{p,s}}} \qquad \ldots \qquad \overset{+2^{2k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{k+1}}{\boxed{0}} \; \overset{+2^{k}}{\boxed{l_{p,1}}} \qquad \overset{+2^{k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{1}}{\boxed{0}} \; \overset{+2^{0}}{\boxed{l_{p,0}}}$$

And lastly, L_{j+1}^* in base Q and base 2 is

$$= \quad \overset{\times Q^{s+1}}{\boxed{0}} \qquad \overset{\times Q^{s}}{\boxed{l_{j+1,s}}} \qquad \ldots \qquad \overset{\times Q^{1}}{\boxed{l_{j+1,1}}} \qquad \overset{\times Q^{0}}{\boxed{l_{j+1,0}}}$$

$$= \quad \overset{+2^{(s+2)k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{(s+1)k+1}}{\boxed{0}} \; \overset{+2^{(s+1)k}}{\boxed{0}} \qquad \overset{+2^{(s+1)k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{sk+1}}{\boxed{0}} \; \overset{+2^{sk}}{\boxed{l_{j+1,s}}} \qquad \ldots \qquad \overset{+2^{2k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{k+1}}{\boxed{0}} \; \overset{+2^{k}}{\boxed{l_{j+1,1}}} \qquad \overset{+2^{k-1}}{\boxed{0}} \; \overset{\ldots}{\boxed{0}} \; \overset{+2^{1}}{\boxed{0}} \; \overset{+2^{0}}{\boxed{l_{j+1,0}}}$$

Then we can see that when QL_j^*, L_p^*, and L_{j+1}^* are written in base 2, any $l_{j,t}$ lines up with $l_{p,t+1}$ and $l_{j+1,t+1}$. Therefore, for any t such that $l_{j,t} = 1$, the condition $QL_j^* \preceq L_p^* + L_{j+1}^*$ guarantees that either $l_{p,t+1} = 1$ or $l_{j+1,t+1} = 1$ (we know from a previous condition that they cannot both be 1).

Next, we will see that the condition $QL_j^* \preceq L_{j+1}^* + QI - 2R_j^*$ specifies that if $r_{i,t} = 0$, then it is $l_{p,t+1} = 1$, whereas if $r_{i,t} \neq 0$, then it is $l_{j+1,t+1} = 1$. First, we know that QI in base Q and base 2 is

	$\times Q^{s+1}$		$\times Q^s$		...		$\times Q^1$		$\times Q^0$
=	1		1		...		1		0

	$+2^{(s+2)k-1}$	...	$+2^{(s+1)k+1}$	$+2^{(s+1)k}$	$+2^{(s+1)k-1}$	...	$+2^{sk+1}$	$+2^{sk}$	...	$+2^{2k-1}$	...	$+2^{k+1}$	$+2^k$	$+2^{k-1}$	...	$+2^1$	$+2^0$
=	0	0	0	1	0	0	0	1	...	0	0	0	1	0	0	0	0

Then recall that in our first condition, we set $r_{i,t} < \frac{Q}{2}$, so any $2r_{i,t} < Q$. Further, note that any value $2r_{i,0}$, $2r_{i,1}$, ..., $2r_{i,s}$ is divisible by 2, so any of these values written out in base 2 will have a coefficient of 0 on the term 2^0. Thus, the value $2R_j^*$ in base 2 has a coefficient of 0 on all 2^0, 2^k, 2^{2k}, ..., 2^{sk}. In particular, $2R_i^*$ in base Q and base 2 is

	$\times Q^{s+1}$		$\times Q^s$		...		$\times Q^1$		$\times Q^0$
=	0		$2r_{i,s}$		...		$2r_{i,1}$		$2r_{i,0}$

	$+2^{(s+2)k-1}$	...	$+2^{(s+1)k+1}$	$+2^{(s+1)k}$	$+2^{(s+1)k-1}$	...	$+2^{sk+1}$	$+2^{sk}$	...	$+2^{2k-1}$	...	$+2^{k+1}$	$+2^k$	$+2^{k-1}$	...	$+2^1$	$+2^0$
=	0	0	0	0	?	?	?	0	...	?	?	?	0	?	?	?	0

Now, suppose that for some t such that $l_{j,t} = 1$, $r_{i,t} = 0$. Then our set up to find the value $L_{j+1}^* + QI - 2R_i^*$ in base 2 will look like one of the following two cases, depending on the specific value of t.

Case A: $t \neq 0$

				$\times 2^{(t+2)k-1}$	...	$\times 2^{(t+1)k+1}$	$\times 2^{(t+1)k}$	$\times 2^{(t+1)k-1}$	...	$\times 2^{tk+1}$	$\times 2^{tk}$	
	L^*_{j+1}	=	...	0	0	0	$l_{j+1,t+1}$	0	0	0	0	...
+	QI	=	...	0	0	0	1	0	0	0	1	...
	$L^*_{j+1} + QI$	=	...	?	?	?	a	0	0	0	1	...
−	$2R^*_j$	=	...	?	?	?	0	0	0	0	0	...
	$L^*_{j+1} + QI - 2R^*_j$	=	...	?	?	?	b	?	?	?	?	...

Case B: $t = 0$

				$\times 2^{2k-1}$	...	$\times 2^{k+1}$	$\times 2^k$	$\times 2^{k-1}$	...	$\times 2^1$	$\times 2^0$
	L^*_{j+1}	=	...	0	0	0	$l_{j+1,t+1}$	0	0	0	0
+	QI	=	...	0	0	0	1	0	0	0	0
	$L^*_{j+1} + QI$	=	...	?	?	?	a	0	0	0	0
−	$2R^*_j$	=	...	?	?	?	0	0	0	0	0
	$L^*_{j+1} + QI - 2R^*_j$	=	...	?	?	?	b	?	?	?	?

In case A, we don't know for certain what the coefficients on any of the terms to the right of 2^{tk} are. So, it is possible that borrowing would have to occur during the subtraction. However, this borrowing will stop at the 2^{tk} column, because the value of $L^*_{j+1} + QI$ here is a 1. In case B, we know no borrowing occurs to the right of $2^{(t+1)k}$, because we can see that all of these coefficients are 0's. Thus, in either case, we know that the coefficients on $2^{(t+1)k}$ remain undisturbed. Further, note that the condition $QL^*_j \preceq L^*_{j+1} + QI - 2R^*_j$ requires that $b = 1$. If $l_{j+1,t+1} = 1$, then $a = 0$, and so $b = 0$, a contradiction to our condition. If $l_{j+t,t+1} = 0$, then $a = 1$, so $b = 1$, as required. Therefore, we can conclude that if $r_{i,t} = 0$, then $l_{j+1,t+1} = 0$, and thus by the condition $QL^*_j \preceq L^*_p + L^*_{j+1}$, $l_{p,t+1} = 1$.

On the other hand, suppose that for t such that $l_{j,t} = 1$, $r_{i,t} \neq 0$. Then again we must consider the following two cases, depending on the specific value of t.

Case A: $t \neq 0$

				$\times 2^{(t+2)k-1}$	...	$\times 2^{(t+1)k+1}$	$\times 2^{(t+1)k}$	$\times 2^{(t+1)k-1}$	...	$\times 2^{tk+1}$	$\times 2^{tk}$	
	L^*_{j+1}	=	...	0	0	0	$l_{j+1,t+1}$	0	0	0	0	...
+												
	QI	=	...	0	0	0	1	0	0	0	1	...
	$L^*_{j+1} + QI$	=	...	?	?	?	a	0	0	0	1	...
−												
	$2R^*_j$	=	...	?	?	?	0	at least one 1			0	...
	$L^*_{j+1} + QI - 2R^*_j$	=	...	?	?	?	b	?	?	?	?	...

Case B: $t = 0$

				$+2^{2k-1}$	...	$+2^{k+1}$	$+2^k$	$+2^{k-1}$	...	$+2^1$	$+2^0$
	L^*_{j+1}	=	...	0	0	0	$l_{j+1,t+1}$	0	0	0	0
+	QI	=	...	0	0	0	1	0	0	0	0
	$L^*_{j+1} + QI$	=	...	?	?	?	a	0	0	0	0
−	$2R^*_j$	=	...	?	?	?	0	at least one 1			0
	$L^*_{j+1} + QI - 2R^*_j$	=	...	?	?	?	b	?	?	?	?

Just as before, in either case, we know that any borrowing that occurs to the right of the 2^{tk} column is stopped at the 2^{tk}. But since $r_{i,t} \neq 0$, we know that at least one of the coefficients on 2^{tk+1}, 2^{tk+2}, ..., $2^{(t+1)k-1}$ in $2R^*_j$ will be a 1. Thus, the borrowing begins again wherever this first 1 is placed, and will continue through to the coefficient of $2^{(t+1)k}$ in $L^*_{j+1} + QI$. If $l_{j+1,t+1} = 1$, then $a = 0$. Then, during borrowing, a will become a 1, making $b = 1$, as required. If $l_{j+1,t+1} = 0$, then $a = 1$. Then, during borrowing, a will become a 0, making $b = 0$, a contradiction to our condition. Thus, if $r_{i,t} \neq 0$, $l_{j+1,t+1} = 1$.

.....

Lastly, we have to make sure that any restrictions L_j of the form $R_i \to R_i + 1$ or $R_i \to R_i - 1$ are followed correctly. In order to do this, we can use the following conditions.

Diophantine Conditions:

For $i = 1$,

$$R^*_i = QR^*_i + \sum_f QL^*_f - \sum_g QL^*_g + x$$

and for $i = 2, 3, ..., n$,

$$R_i^* = QR_i^* + \sum_f QL_f^* - \sum_g QL_g^*$$

where $\sum_f QL_f^*$ is the sum over all f such that $L_f : R_i \to R_i + 1$ and $\sum_g QL_g^*$ is the sum over all g such that $L_g : R_i \to R_i - 1$.

Reasoning: For $i = 2, 3, ..., n$, we can picture the condition $R_i^* = QR_i^* + \sum_f QL_f^* - \sum_g QL_g^*$ as follows:

			$\times Q^{s+1}$	$\times Q^s$		$\times Q^1$	$\times Q^0$
	QR_i^*	=	$r_{i,s}$	$r_{i,s-1}$	...	$r_{i,0}$	0
+							
	QL_{f_1}	=	$l_{f_1,s}$	$l_{f_1,s-1}$	...	$l_{f_1,0}$	0
	$\vdots$				$\vdots$		
+							
	QL_{f_α}	=	$l_{f_\alpha,s}$	$l_{f_\alpha,s-1}$	...	$l_{f_\alpha,0}$	0
−							
	QL_{g_1}	=	$l_{g_1,s}$	$l_{g_1,s-1}$	...	$l_{g_1,0}$	0
	$\vdots$				$\vdots$		
−							
	QL_{g_β}	=	$l_{g_\beta,s}$	$l_{g_\beta,s-1}$	...	$l_{g_\beta,0}$	0
	R_i^*	=	$r_{i,s+1}$	$r_{i,s}$	...	$r_{i,1}$	$r_{i,0}$

Note that this picture would be the same for the condition $R_1^* = QR_1^* + \sum_f QL_f^* - \sum_g QL_g^* + x$, with the addition of x in the Q^0 column.

Then $r_{i,0} = 0$ for all $i = 1, 2, ...n$, and $r_{1,0} = x$, as desired. For any $t \neq 0$, $r_{i,t} = r_{i,t-1} + l_{f_1,t-1} + ... + l_{f_\alpha,t-1} - l_{g_1,t-1} - ... - l_{g_\beta,t-1}$. At time t, if the instruction at time $t-1$ was to add 1 to R_i, then one of the $l_{f_1,t-1}$, ..., $l_{f_\alpha,t-1}$ will be a 1, and $r_{i,t} = r_{i,t-1} + 1$. If the instruction was to subtract 1 from R_i, then one of the $l_{g_1,t-1}$, ..., $l_{g_\beta,t-1}$ will be a 1, and $r_{i,t} = r_{i,t-1} - 1$. For any other type of instruction, $r_{i,t} = r_{i,t-1}$. Thus, our conditions guarantee that each for any time t, each register

has the appropriate entry.

.....

To conclude, given a computably enumerable set S, there must be some register machine M such that M halts on input x if and only if $x \in S$. We have now seen a group of Diophantine conditions that will be satisfied if and only if there is a progression of M that halts on input x. Therefore, these Diophantine conditions are satisfied if and only if $x \in S$, so S is a Diophantine set.

We have now seen that a set is Diophantine if and only if it is computably enumerable. With this result, we can proceed to prove the unsolvability of Hilbert's tenth problem.

Chapter 5

Hilbert's Tenth Problem is Unsolvable

From our background in computability theory, we know that there are many sets which are computably enumerable but not computable. By the remarkable result proved in Chapter 4, we now know that these sets are Diophantine sets that are not computable. Then if we consider the Diophantine equation that represents any such set, we know that there is no process to determine whether or not the eqauation is solvable in the natural numbers. Thus, the process desired by Hilbert does not exist, and his tenth problem is proven unsolvable.

Bibliography

[1] Matiyasevich, Y. *Hilbert's Tenth Problem*. MIT Press, (1993), Massachusetts.

[2] Jones, J.P, and Matiyasevich, Y.V. *Register Machine Proof of the Theorem on Exponential Diophantine Representation of Enumerable Sets*. The Journal of Symbolic Logic, vol. 49, (1984), pp.818-828.