CARLETON UNIVERSITY

SCHOOL OF
MATHEMATICS AND STATISTICS

HONOURS PROJECT

TITLE: Hilbert's Tenth Problem

AUTHOR: Brandon Savage-Barnhart

SUPERVISOR: Brandon Fodden

DATE: January 8, 2020

Section 1: Diophantine Equations and Sets

The focus of this paper, Hilbert's tenth problem, asks whether there exists an algorithm that can determine the existence of integer solutions for a given polynomial with integer coefficients. As the name suggests, the problem was the tenth in a famous list of twenty-three questions that mathematician David Hilbert posed at the 1900 International Congress of Mathematicians. These types of polynomials, such that both the coefficients and the desired solutions are integers, are properly referred to as ***Diophantine equations*** after the mathematician Diophantus of Alexandria of the third century BC.

Diophantus' study of algebraic equations was expansive and thorough, providing inspiration for mathematicians across Europe until at least the 1600s (see [H] for more about Diophantus' legacy). As a result, the study of Diophantine equations and their solutions is known today as ***Diophantine analysis***, and ranges from simple examples known since antiquity such as the *Pythagorean triples* (integer solutions to the equation $x^2 + y^2 = z^2$) to more complicated equations like $x^2 = 61y^2 + 1$. This latter equation is an example of a ***Pell equation*** and remains notable for having first been solved by Indian mathematicians hundreds of years before a solution was found in Europe using more complicated methods. In modern mathematics, it is commonplace for one to exhaust every tool and resource at their disposal to solve a problem; this includes, but is not limited to, reframing problems through different fields or equivalent expressions to apply theorems previously inaccessible.

For instance, at the time of Hilbert's conference, there had already existed a tool that could narrow the problem to solutions in terms of ***natural numbers*** *(defined as the set of positive integers, without zero).* 130 years earlier, Joseph Louis Lagrange provided the first proof of a theorem now known as ***Lagrange's four-square theorem*** (stated below, see Theorem 3.15 of [MF] for a proof) that Claude Gaspard Bachet de Méziriac had posited in the margins of his Latin translation of Diophantus' *Arithmetica*; it is believed that Diophantus himself was aware of such a theorem, as evidenced by examples within the *Arithmetica.*

Lagrange's four-square theorem: Every non-negative integer can be written as a sum of four squares.

Using Lagrange's four-square theorem, it will be shown that considering only the natural number solutions of a given polynomial with integer coefficients is actually an equivalent problem to the one described by Hilbert. Then by understanding which sets of ordered n-tuples of natural numbers correspond to Diophantine equations, and in turn which natural number-valued functions satisfy the construction of these sets, it will then be possible to construct a function in such a manner that it must be that Hilbert's tenth problem is unsolvable. The first proof of this result was demonstrated by Yuri Matiyasevich in 1970, building on earlier results from Martin Davis, Julia Robinson and Hilary Putnam.

Given a Diophantine equation $P(x_1, \dots, x_n)$ along with an arbitrary natural number solution $(x_1, \dots, x_n)$, there exists an equivalent integer solution of a Diophantine equation P' determined by using Lagrange's four-square theorem and rewriting each natural number x_j as a sum of four integer squares:

$$\boldsymbol{x_j = 1 + p_j^2 + q_j^2 + r_j^2 + s_j^2}, \text{ for } \boldsymbol{j = 1, \dots n},$$

so that: $$\boldsymbol{P(x_1, \dots, x_n) = 0 \leftrightarrow P'(p_1, q_1, r_1, s_1, \dots, p_n, q_n, r_n, s_n) = 0}.$$

Therefore if an algorithm can determine whether $P'(p_1, q_1, r_1, s_1, \dots, p_n, q_n, r_n, s_n) = 0$ has an integer solution, such as the one described by Hilbert's tenth problem, then it would be able to determine a natural number solution to the Diophantine equation $P(x_1, \dots, x_n) = 0$.

It is simple to show the converse, that any algorithm that can determine natural number solutions of a given Diophantine equation would also be able to determine integer solutions. Given a Diophantine equation $Q(x_1, \dots, x_n)$ along with an arbitrary integer solution $(x_1, \dots, x_n)$, there exists an equivalent natural number solution of a Diophantine equation Q' determined by rewriting each integer x_j as the difference of two natural numbers y_j and z_j:

$$\boldsymbol{x_j = y_j - z_j}, \text{ for } \boldsymbol{j = 1, \dots n},$$

so that: $$\boldsymbol{Q(x_1, \dots, x_n) = 0 \leftrightarrow Q'(y_1, z_1, \dots, y_n, z_n) = 0}.$$

Therefore if an algorithm can determine whether $Q'(y_1, z_1, \dots, y_n, z_n) = 0$ has a natural number solution, it would be capable of determining integer solutions for $Q(x_1, \dots, x_n) = 0$. Combining this result with the previous one, finding an algorithm that can determine the existence of a natural number solution for a given Diophantine equation is an equivalent problem to the one described by Hilbert's tenth problem. Using this fact, in the work that follows, only positive integer solutions of Diophantine equations with integer coefficients will be discussed.

Building on the foundation established above, Hilbert's tenth problem can be reframed in the following manner; as opposed to seeking the solutions for a given Diophantine equation, a set of positive-integer n-tuples is instead treated as a solution set with the goal of finding a corresponding Diophantine equation. All of these results can be summarized in the following definition:

Definition: A set D of ordered n-tuples of natural numbers is called a **Diophantine set** if there exists a Diophantine equation $P(x_1, \dots, x_n, y_1, \dots, y_m)$, with $m \geq 0$ such that the following holds:

$$\boldsymbol{(x_1, \dots, x_n) \in D \leftrightarrow (\exists y_1, \dots, y_m)[P(x_1, \dots, x_n, y_1, \dots, y_m) = 0]}.$$

One question that might come to mind is, "Which sets are Diophantine?" It turns out that quite a number of well-known sets are Diophantine, such as the set of composite numbers. A few simple examples are presented below to demonstrate their construction:

The set of even numbers:	$\boldsymbol{x \in D \leftrightarrow (\exists y)\,[x - 2y = 0]}$.
The set of composite numbers:	$\boldsymbol{x \in D \leftrightarrow (\exists y, z)\,[x - (y+1)(z+1) = 0]}$.
The set of numbers not divisible by 3:	$\boldsymbol{x \in D \leftrightarrow 3 \nmid x \leftrightarrow 3 \mid (x+1)}$ **or** $\boldsymbol{3 \mid (x-1)}$,
	$\boldsymbol{\leftrightarrow 3 \mid (x+1)(x-1) \leftrightarrow 3 \mid (x^2 - 1) \leftrightarrow (\exists y)[x^2 - 1 - 3(y-1) = 0]}$.
The set of *Pythagorean triples*:	$\boldsymbol{(x, y, z) \in D \leftrightarrow [x^2 + y^2 - z^2 = 0]}$.

Notice in the third example above, to satisfy the case when $x = 1$, the factor $y - 1$ is used so that all variables defined are natural numbers. The fourth example demonstrates a multivariable Diophantine set, and leads into the next set of examples. By considering multiple variables in an expression, the following examples demonstrate how some relations can yield Diophantine sets, such as the divisibility and ordering relations.

The divisibility relation, $\boldsymbol{x \mid y}$, is Diophantine:	$\boldsymbol{(x, y) \in D \leftrightarrow x \mid y \leftrightarrow (\exists z)\,[xz - y = 0]}$.
The ordering relation, $\boldsymbol{x < y}$, is Diophantine:	$\boldsymbol{(x, y) \in D \leftrightarrow x < y \leftrightarrow (\exists z)\,[y - z - x = 0]}$.
The combined relation, $\boldsymbol{x \mid y}$ and $\boldsymbol{x < z}$:	$\boldsymbol{(x, y, z) \in D \leftrightarrow (\exists u, v)[(xu - y)^2 + (z - v - x)^2 = 0]}$.

The latter result demonstrates how known Diophantine sets can be used to construct other Diophantine sets. Given two Diophantine sets, A and B, along with their respective Diophantine equations P_A, P_B:

$$\boldsymbol{x \in A \cup B \leftrightarrow x \in A \; or \; x \in B \leftrightarrow P_A P_B = 0}$$
$$\boldsymbol{x \in A \cap B \leftrightarrow x \in A \; and \; x \in B \leftrightarrow {P_A}^2 + {P_B}^2 = 0}.$$

The former is referred to as the ***disjunction*** of the two expressions $x \in A$ and $x \in B$ while the latter is referred to as the ***conjunction***; in particular, the technique used for the conjunction will be referred to in later sections as the *summation of squares*.

The congruence relation, $x \equiv y \; (mod\; z)$, is Diophantine: $\boldsymbol{(x, y, z) \in D \leftrightarrow z \mid x - y}$,
$\boldsymbol{\leftrightarrow (\exists w)(x - y = (w-1)z \; or \; y - x = (w-1)z) \leftrightarrow [(x - y - (w-1)z)(y - x - (w-1)z) = 0]}$.

These techniques provide inspiration for the following definition, which focuses on the logical operations that preserve the Diophantine nature of sets.

Definition: A logical connective that can be applied to a known Diophantine set to yield another Diophantine set is called a ***Diophantine predicate***.

Clearly the logical connectives "AND" (^) and "OR" (∨) are Diophantine predicates, using the general methods provided earlier. This can be extended inductively, given a finite number of Diophantine expressions, the conjunction as well as the disjunction of these expressions are both Diophantine. The following example demonstrates that "THERE EXISTS" (∃) is also a Diophantine predicate.

Consider the set $D = \{(x, y) | x - 2y = 0\}$, which is clearly Diophantine. Then the set of even numbers, briefly seen earlier, can alternatively be defined as $\{x | (\exists y)\ such\ that\ (x, y) \in D\}$.

Logical connectives such as "NOT" (∼), "FOR ALL" (∀), and "IF, THEN" (→) may or may not preserve whether sets are Diophantine. There does exist another Diophantine predicate, known as the ***bounded universal quantifier***, which provides a bounded application of the "FOR ALL" (∀) connective. However, it will be formally defined in the next section when the tools necessary to prove it are provided.

The following theorem, first proved by Hilary Putnam, demonstrates another relationship between Diophantine sets and polynomials.

Theorem 1.1: Let S be a set of natural numbers. Then:

$\boldsymbol{S}$ **is Diophantine** ↔ ∃ **a polynomial** $\boldsymbol{P}$ **such that** $\boldsymbol{S}$ **is the set of natural numbers in the range of** $\boldsymbol{P}$.

Proof (←): Clearly, if there exists a polynomial $P(x_1, \dots, x_m)$ with a range that includes at least one natural number, then one can define the polynomial $Q(x, x_1, \dots, x_m) = P(x_1, \dots, x_m) - x$. Then the set of natural numbers in the range of P, now denoted S, is Diophantine since:

$$x \in S \leftrightarrow (\exists x_1, \dots, x_m)[Q(x, x_1, \dots, x_m) = 0].$$

Proof (→): Suppose that S is Diophantine, meaning that there exists a polynomial Q such that:

$$x \in S \leftrightarrow (\exists x_1, \dots, x_m)[Q(x, x_1, \dots, x_m) = 0].$$

Now let $\boldsymbol{P(x, x_1, \dots, x_m) = x\left[1 - Q^2(x, x_1, \dots, x_m)\right]}$; it will be shown that $x \in S$ if and only if x is a natural number in the range of P.

If $x \in S$, then $\exists x_1, \dots, x_m$ such that $Q(x, x_1, \dots, x_m) = 0 \rightarrow Q^2(x, x_1, \dots, x_m) = 0$. Therefore, it must be that $\boldsymbol{P(x, x_1, \dots, x_m) = x(1 - 0) = x}$, and so x is in the range of P.

Conversely, suppose that $z = P(x, x_1, \dots, x_m)$ with $z > 0$. Since x is a natural number, it must be that the factor $1 - Q^2(x, x_1, \dots, x_m)$ is positive. This can only be true if Q vanishes at $(x, x_1, \dots, x_m)$, meaning that $Q(x, x_1, \dots, x_m) = 0$. Therefore, $x \in S$ and $z = x$. ■

Consider the set of composite numbers S, with $Q(x, y, z) = x - (y + 1)(z + 1)$. Then the positive range of the polynomial $P(x, y, z) = x[1 - (x - (y + 1)(z + 1))^2]$ is precisely the set S.

Section 2: Diophantine Functions

This section will focus on expanding the Diophantine concepts introduced in the previous section to functions, particularly natural number-valued functions of one or more natural number arguments. Note that the notation $\mathbb{N}_n$ refers to the collection of all sets of n-tuples of natural numbers. In this approach, a function is said to be Diophantine if its graph is Diophantine.

Definition: A function $f: \mathbb{N}_n \to \mathbb{N}$ is **Diophantine** if the set $\{(x_1, \dots, x_n, f(x_1, \dots, x_n))\}$ is Diophantine.

Applying and extending the Diophantine concepts to the study of functions, similar to in Section 1 with sets, one might wonder which functions in particular are Diophantine. A few simple examples are presented below to demonstrate how it might be shown that a function is Diophantine:

The doubling function: $f(x) = 2x,\ x \in \mathbb{N}$, is a Diophantine function,
$\leftrightarrow D = \{(x, 2x) | x \in \mathbb{N}\}$ is a Diophantine set, and $\big((x, y) \in D \leftrightarrow y - 2x = 0\big)$.

The additive function: $f(x, y) = x + y,\ x, y \in \mathbb{N}$, is a Diophantine function,
$\leftrightarrow D = \{(x, y, x + y) | x, y \in \mathbb{N}\}$ is a Diophantine set, and $\big((x, y, z) \in D \leftrightarrow z - y - x = 0\big)$.

The multiplicative function: $f(x, y) = xy,\ x, y \in \mathbb{N}$, is a Diophantine function,
$\leftrightarrow D = \{(x, y, xy) | x, y \in \mathbb{N}\}$ is a Diophantine set, and $\big((x, y, z) \in D \leftrightarrow z - xy = 0\big)$.

Similar to Section 1, determining whether or not a given function is Diophantine still depends largely on finding an explicit Diophantine equation. As a result, while the definition helps extend some of the concepts seen earlier to the field of functions, it doesn't do as much to help understand why certain sets or functions are Diophantine without proof. The usefulness of this extension is that it will enable the construction of specific Diophantine functions that will aid in the proof of Hilbert's tenth problem, in particular the ***Sequence Number Function***.

The *Sequence Number Function* encodes all finite sequences of natural numbers within a single function. This powerful result follows from clever use of the famous ***Chinese Remainder Theorem*** and was first demonstrated by the mathematician Kurt Gödel in the proof of his two famous *incompleteness theorems*.

Using the *Sequence Number Function*, along with a number of other Diophantine functions and results, it will finally be possible to explicitly determine all functions that are Diophantine. Furthermore, this will enable the construction of sets and functions designed to disprove Hilbert's tenth problem. Constructing this function however, requires looking at the set of *triangular numbers* as well as using them to form a bijection between the natural numbers $\mathbb{N}$ and $\mathbb{N}_2$.

Consider the ***triangular numbers***, defined for all natural numbers k as the sum of all integers from 1 to k.

$$\boldsymbol{T(k) = 1 + 2 + \cdots + k = \frac{k(k+1)}{2}}.$$

Clearly the triangular numbers are an increasing function; therefore, for every natural number z, there exists a unique nonnegative integer n such that $\boldsymbol{T(n) < z \leq T(n+1) = T(n) + (n+1)}$.

It follows that	$(\forall \boldsymbol{z})\ \boldsymbol{z = T(n) + y}$, where $0 < y \leq n + 1$,
and therefore	$(\forall \boldsymbol{z})\ \boldsymbol{z = T(x + y - 2) + y}$, where $x + y = n + 2$.

The variables x, y are uniquely determined for all z as above, creating a bijection between the natural numbers and the pairs of natural numbers. For each z, two functions $L(z)$ and $R(z)$ can be defined to represent the variables x and y respectively. That is,

$$\boldsymbol{x = L(z) \leftrightarrow (\exists y)\ [2z = (x + y - 2)(x + y - 1) + 2y]},$$
$$\boldsymbol{y = R(z) \leftrightarrow (\exists x)\ [2z = (x + y - 2)(x + y - 1) + 2y]}.$$

Conversely, given a pair of natural numbers x and y, one can define a function $z = P(x, y)$ by setting $P(x, y) = T(x + y - 2) + y$. That is,

$$\boldsymbol{z = P(x, y) \leftrightarrow 2z = (x + y - 2)(x + y - 1) + 2y}.$$

By substituting $P(x, y)$ for z in the definitions of $L(z)$ and $R(z)$ given above, the left sides of the equations present that $\boldsymbol{L\big(P(x, y)\big) = x}$ and $\boldsymbol{R\big(P(x, y)\big) = y}$. In a similar vein, substituting $L(z)$ and $R(z)$ for x and y respectively in the definition of $P(x, y)$ yields the relation $\boldsymbol{z = P\big(L(z), R(z)\big)}$.

From this, it can now be understood that the functions $L(z)$ and $R(z)$ denote left and right respectively, while the function $P(x, y)$ refers to the pair of integers. These results can be summarized in the following theorem.

Pairing Function Theorem *(Theorem 2.1)***:** The functions $L(z), R(z)$ and $P(x, y)$ are Diophantine functions such that $P\colon \mathbb{N}_2 \to \mathbb{N}$ is a bijection. Moreover, the following results hold for all $x, y, z \in \mathbb{N}$:

(1): $$L\big(P(x, y)\big) = x, R\big(P(x, y)\big) = y.$$

(2): $$P\big(L(z), R(z)\big) = z, \text{ with } L(z), R(z) \leq z.$$

The relation between the functions $L(z)$, $R(z)$ and $P(x, y)$ can be illustrated in the following chart.

		$\boldsymbol{R(z)}$					
		1	**2**	**3**	**4**	**5**	**6**
$\boldsymbol{L(z)}$	**1**	1	3	6	10	15	21
	2	2	5	9	14	20	27
	3	4	8	13	19	26	34
	4	7	12	18	25	33	42
	5	11	17	24	32	41	51
	6	16	23	31	40	50	61

For example, suppose $z = 16$. Locating 16 in the body of the above chart, that implies $L(z) = 6$ and $R(z) = 1$ and from the definition of the function $P(x, y)$, $P(6,1) = 16$.

Using the two functions $L(z)$ and $R(z)$, it is now possible to construct and define the ***Sequence Number Function*** as follows:

$\boldsymbol{S(i,u) = w}$, where $\boldsymbol{w \equiv L(u)\ (mod\ 1 + iR(u))}$ and $\boldsymbol{1 \leq w \leq 1 + iR(u)}$.

Suppose $u = 5$. Looking at the chart, $L(5) = 2$ and $R(5) = 2$. Then:

$$\boldsymbol{S(i,5) \equiv 2\ (mod\ 1 + 2i) \rightarrow S(1,5) = 2, S(2,5) = 2, \ldots}$$

Thus, every constant sequence consisting solely of the value 2 is encoded by setting $u = 5$.

Suppose $u = 16$. Looking at the chart, $L(16) = 6$ and $R(16) = 1$. Then:

$$\boldsymbol{S(i,16) \equiv 6\ (mod\ 1 + i) \rightarrow} \begin{cases} S(1,16) = 2, & S(2,16) = 3, \\ S(3,16) = 2, & S(4,16) = 1, \\ S(5,16) = 6, & S(6,16) = 6, \ldots \end{cases}$$

Thus the sequences $\{2\}, \{2,3\}, \{2,3,2\}$ and $\{2,3,2,1\}$, along with every finite sequence of natural numbers beginning $\{2,3,2,1\}$ followed only by 6s until the sequence terminates, are all encoded by setting $u = 16$.

As mentioned earlier, the *Sequence Number Function* encodes all finite sequences of natural numbers within a single function. Moreover, from its construction, it can be shown that the *Sequence Number Function* is a Diophantine function.

Theorem 2.2: The function $S(i,u)$ is Diophantine, with $S(i,u) \leq u$. Furthermore:

For every sequence of natural numbers $a_1, \dots, a_n$, there exists a natural number u such that:

$$S(i,u) = a_i \text{ for all } 1 \leq i \leq n.$$

Proof: Clearly $S(i,u) \leq L(u) \leq u$. Now consider the following three equations:

(1) $$\boldsymbol{2u = (x+y-2)(x+y-1)+2y}$$

(2) $$\boldsymbol{w+v-1 = 1+iy} \leftrightarrow w \leq 1+iy$$

(3) $$\boldsymbol{w-x = z(1+iy)} \leftrightarrow w - x \equiv 0 \ (mod\ 1+iy)$$

The first equation implies $u = P(x,y)$, and hence $x = L(u)$ and $y = R(u)$, while the combination of the three assert the claim that $w = S(i,u)$. By taking the summation of the squares of each equation, it is clear that $S(i,u)$ is Diophantine. To prove the second part of the theorem, the following theorem is required (see Theorem 3.12 of [MF] for a proof):

Chinese Remainder Theorem: Let $b_1, \dots, b_n, m_1, \dots, m_n$ be natural numbers such that:

$(*)$ $i \neq j \rightarrow m_i \text{ and } m_j$ are relatively prime.

Then there exists a natural number x such that $\boldsymbol{x \equiv b_1\ (mod\ m_1) \equiv \cdots \equiv b_n\ (mod\ m_n)}$.

Let $a_1, \dots, a_n$ be natural numbers, and choose y to be an integer greater than each of $a_1, \dots, a_n$ and divisible by each of $1,2, \dots, n$. Then $\{m_1 = 1+y, m_2 = 1+2y, \dots, m_n = 1+ny\}$ satisfies $(*)$.

To show this, suppose a prime p divides both m_i and m_j. Without loss of generality, assume $i < j$.

Then $\boldsymbol{p \big| (m_j - m_i) \rightarrow p \big| \big((1+jy) - (1+iy)\big) \rightarrow p | (j-i)y}$.

Suppose p does not divide y, so p must divide $j - i < n$. Then by definition of y, p divides y. As a result, p must divide $\boldsymbol{m_j - jy = (1+jy) - jy = 1}$. Thus, $p = 1$ and the set $\{\boldsymbol{m_i = 1+iy | 1 \leq i \leq n}\}$ satisfies $(*)$.

Therefore, applying the ***Chinese Remainder Theorem*** yields a number x such that:

$$\boldsymbol{x \equiv a_1\ (mod\ 1+y) \equiv \cdots \equiv a_n\ (mod\ 1+ny)}$$

Finally, let $u = P(x,y) \rightarrow x = L(u), y = R(u)$. Then $\forall i$ with $1 \leq i \leq n, a_i \equiv L(u)\ \big(mod\ 1 + iR(u)\big)$.

Thus, by definition, $S(i,u) = a_i$ for all $1 \leq i \leq n$. ■

The above result is an incredibly powerful tool, crucial to determining the construction of all Diophantine functions as will be shown in the next section. Even for a small sequence of natural numbers, the value of the x satisfying all of the congruences can be quite large. That being said, using the following example to demonstrate, it is simple to generate an algorithm that can determine the values of x and u.

Consider the sequence of natural numbers $\boldsymbol{a_1 = 5, a_2 = 6, a_3 = 7}$. Following the methods used in the proof of Theorem 2.2, an integer y must be chosen such that y is greater than each of a_1, a_2, and a_3 as well as divisible by 1, 2 and 3. Therefore, the smallest possible value that can be chosen is $\boldsymbol{y = 12}$. From the proof of Theorem 2.2, this implies that $\boldsymbol{m_1 = 13, m_2 = 25}$ and $\boldsymbol{m_3 = 37}$ are relatively prime, and by the *Chinese Remainder Theorem*, there exists a natural number x such that:

$$\boldsymbol{x \equiv 5\ (mod\ 13) \equiv 6\ (mod\ 25) \equiv 7\ (mod\ 37).}$$

To solve this system of congruences, consider that $\boldsymbol{2(13) + 5 = 31 = 1(25) + 6}$. Thus, the first two congruences can be satisfied by setting $\boldsymbol{x_0 = 31}$. The third congruence is obviously unsatisfied, as the smallest two natural numbers congruent to 7 modulo 37 are 44 and 7 itself, however solving the three together is a simple matter of searching the values which satisfy the first two congruences and checking the third. Explicitly, this means one can simply add the *lowest common multiple* of the two moduli, 13 and 25, to the initial value $x_0 = 31$ to find other solutions of the first two congruences.

In this example, and in general since the moduli were shown to always be relatively prime to one another, the lowest common multiple of 13 and 25 is equal to the product $13 \cdot 25 = 325$. Since 325 and 37 are also relatively prime, the remainder of 325 divided by 37 (which is 29) must be relatively prime to 37, and so the third congruence will eventually be satisfied by adding in increments of 325:

$$\begin{aligned}
\boldsymbol{x_0 = 31 \equiv 5\ (mod\ 13) \equiv 6\ (mod\ 25) \equiv 31\ (mod\ 37)},\\
\boldsymbol{31 + 325 = 356 \equiv 5\ (mod\ 13) \equiv 6\ (mod\ 25) \equiv 23\ (mod\ 37)},\\
\boldsymbol{356 + 325 = 681 \equiv 5\ (mod\ 13) \equiv 6\ (mod\ 25) \equiv 15\ (mod\ 37)},\\
\boldsymbol{681 + 325 = 1006 \equiv 5\ (mod\ 13) \equiv 6\ (mod\ 25) \equiv 7\ (mod\ 37)}.
\end{aligned}$$

Thus, the value $\boldsymbol{x = 1006}$ satisfies the three congruences. Finally, since $x = 1006$ and $y = 12$, plugging into the equation for $P(x, y)$ yields $\boldsymbol{u = P(1006, 12) = 516648}$. In general, given a sequence of natural numbers, one can determine the value of y and solve at least one of the congruences produced by the *Chinese Remainder Theorem*. Then inductively, by adding the *lowest common multiple* of the moduli of the congruences already solved, the rest of the potential solutions can be quickly found and checked. It can be rigorously shown that this procedure will always work and it should be noted that every sequence of natural numbers will yield multiple natural numbers that satisfy all required congruences.

In 1931, Kurt Gödel provided a similar function that could encode all finite sequences of natural numbers $a_1, \dots, a_n$. In his explanation, he described the natural number u satisfying $S(i,u) = a_i$ now referred to as the ***Gödel number*** of the sequence. Furthermore, Gödel's construction also involves taking the smallest satisfying value for u, guaranteeing uniqueness. In the example provided earlier, for instance, the Gödel number of the sequence 5, 6 and 7 is 516648.

The following definition is not nearly as potent, but is critical for showing that other common integer-valued functions are Diophantine.

Definition: The **floor function,** $[\ \ ]: \mathbb{R} \to \mathbb{Z}$, is defined for all real numbers α to be the unique integer $[\alpha]$ satisfying:

$$[\boldsymbol{\alpha}] \leq \boldsymbol{\alpha} < [\boldsymbol{\alpha}] + \mathbf{1}.$$

It is important to note that the floor function is not a function defined only for natural number inputs and outputs such as was specified at the beginning of this section. However, its use in Theorem 2.4 to prove that other natural number-valued functions are Diophantine will be in conjunction with expressions that guarantee a natural number output. First, the following lemma is required.

Lemma 2.3: For $\boldsymbol{0 < k \leq n, u > 2^n}$: $\left[\frac{(u+1)^n}{u^k}\right] = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}$.

Proof: By expanding the polynomial, it can be observed that:

$$\frac{(u+1)^n}{u^k} = \sum_{i=0}^{n} \binom{n}{i} u^{i-k} = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} + \sum_{i=k}^{n} \binom{n}{i} u^{i-k}.$$

Define the term on the left to be $\boldsymbol{R} = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}$ and the term on the right to be $\boldsymbol{S} = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}$. Note that S is in fact an integer, since for every $k \leq i \leq n$, the value of u^{i-k} is as well. Then:

$$R < u^{-1} \sum_{i=0}^{k-1} \binom{n}{i} < u^{-1} \sum_{i=0}^{n} \binom{n}{i} = u^{-1}(1+1)^n < 1.$$

It immediately follows that $S \leq \frac{(u+1)^n}{u^k} < S + 1$, and so the floor of $\frac{(u+1)^n}{u^k}$ is $R = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}$. ■

One can now show that the ***exponential function***, $\boldsymbol{h(n,k) = n^k}$ is a Diophantine function. Although it will simply be assumed for now, after proving the result to Hilbert's tenth problem, the result will be explored and proven (*Theorem 5.14*). With the assumption that the exponential function is Diophantine, along with the lemma above, it can be shown that the following functions are Diophantine.

Theorem 2.4: The following functions are Diophantine:

(1) $$\boldsymbol{f(n,k) = \binom{n}{k}},$$

(2) $$\boldsymbol{g(n) = n!},$$

(3) $$\boldsymbol{h(a,b,y) = \prod_{k=1}^{y}(a+bk)}.$$

Proof: Take $0 < k \leq n$ and $u > 2^n$. By the previous lemma, it follows that $\left[\frac{(u+1)^n}{u^k}\right] \equiv \binom{n}{k} \ (mod\ u)$. Since $\binom{n}{k} \leq \sum_{i=0}^{n}\binom{n}{i} = 2^n < u$, it follows that $\binom{n}{k}$ is the unique positive integer congruent to $\left[\frac{(u+1)^n}{u^k}\right]$ modulo u. Thus:

$$\boldsymbol{z = \binom{n}{k} \leftrightarrow (\exists u,v,w)(v = 2^n)\wedge(u > v)\wedge\left(w = \left[\frac{(u+1)^n}{u^k}\right]\right)\wedge\big(z \equiv w\ (mod\ u)\big)\wedge(z < u)}.$$

It is claimed that this is a conjunction of Diophantine expressions. The exponential function is simply assumed for now to be Diophantine; although capable of proving it now, the result is lengthy and will be explored properly in Section 5. The inequality $\boldsymbol{v < u}$ is clearly Diophantine, as shown in the examples provided in Section 1. For the expression $\boldsymbol{w = \left[\frac{(u+1)^n}{u^k}\right]}$, consider the following:

$$\boldsymbol{w = \left[\frac{(u+1)^n}{u^k}\right] \leftrightarrow (\exists x,y,t)(t = u+1)\wedge(x = t^n)\wedge(y = u^k)\wedge(w \leq \frac{x}{y} < w+1)}.$$

This is clearly a conjunction of Diophantine expressions, and so the left side is as well. Recall it was shown that the congruence relation is a Diophantine relation. Then consider the following:

$$\boldsymbol{\big(z \equiv w\ (mod\ u)\big)\wedge(z < u) \leftrightarrow (\exists x,y)(w = z + (x-1)u)\wedge(u = z + y)}.$$

Thus $f(n,k)$ is Diophantine.

For $r > (2n)^{n+1}$, it can be shown that $n! = \left[r^n \Big/ \binom{r}{n}\right]$ (see Lemma 4.4 of [D] for proof).

Then in a manner similar to above, it follows that $g(n) = n!$ can be expressed as a conjunction of Diophantine expressions.

Finally, to show that $h(a,b,y)$ is Diophantine, suppose that $bq \equiv a\ (mod\ M)$. Then $b^y y!\binom{q+y}{y} = b^y(q+y)(q+y-1)\ldots(q+1) = (bq+yb)(bq+(y-1)b)\ldots(bq+b)$, which is congruent modulo M to $(a+yb)(a+(y-1)b)\ldots(a+b) = \prod_{k=1}^{y}(a+bk) = h(a,b,y)$.

It can be shown that with the proper choice of M, the congruence $bq \equiv a\ (mod\ M)$ will always have a solution for a given $a,b \in \mathbb{N}$ (see Lemma 4.7 of [D] for proof) and so $h(a,b,y)$ is Diophantine. ■

One of the results that follows from this theorem is the *bounded universal quantifier*, briefly mentioned in Section 1 as a Diophantine predicate that provides a limited application of the "FOR ALL" (∀) quantifier. With the theorems covered in Section 2 however, one can now prove that it is indeed a Diophantine predicate. As such, there is the following definition:

Definition: The **bounded universal quantifier** is defined as follows: $(\forall \boldsymbol{z})_{\leq \boldsymbol{y}} \ldots = (\forall \boldsymbol{z})(\boldsymbol{z} > \boldsymbol{y}) \vee (\ldots)$.

Along with the definition, there is the following theorem.

Theorem 2.5: If P is a Diophantine equation, define the following set:

$$\boldsymbol{S} = \left\{(\boldsymbol{y}, \boldsymbol{x_1}, \ldots, \boldsymbol{x_n}) \middle| (\forall \boldsymbol{z})_{\leq \boldsymbol{y}} (\exists \boldsymbol{y_1}, \ldots, \boldsymbol{y_m}) \; [\boldsymbol{P}(\boldsymbol{y}, \boldsymbol{z}, \boldsymbol{x_1}, \ldots, \boldsymbol{x_n}, \boldsymbol{y_1}, \ldots, \boldsymbol{y_m}) = \boldsymbol{0}]\right\}.$$

Then S is a Diophantine set.

Davis gives a Diophantine definition of S (see [D], Theorem 5.1) consisting of a long conjunction of exponential functions along with functions already shown to be Diophantine. The proof is long and tedious, and is omitted here. Using the *bounded universal quantifier*, it is now possible to show that even more sets are Diophantine. For example:

The set of prime numbers:
$$\boldsymbol{x} \in \boldsymbol{D} \leftrightarrow (\forall \boldsymbol{y})_{\leq \boldsymbol{x}} (\forall \boldsymbol{z})_{\leq \boldsymbol{x}} [(\boldsymbol{y} = \boldsymbol{1}) \vee (\boldsymbol{z} = \boldsymbol{1}) \vee (\boldsymbol{yz} < \boldsymbol{x}) \vee (\boldsymbol{yz} > \boldsymbol{x})],$$
$$\leftrightarrow (\forall \boldsymbol{y})_{\leq \boldsymbol{x}} (\forall \boldsymbol{z})_{\leq \boldsymbol{x}} (\exists \boldsymbol{k}) \big((\boldsymbol{y} - \boldsymbol{1})(\boldsymbol{z} - \boldsymbol{1})(\boldsymbol{x} - \boldsymbol{yz} - \boldsymbol{k})(\boldsymbol{yz} - \boldsymbol{x} - \boldsymbol{k}) = \boldsymbol{0}\big).$$

Recall Theorem 1.1, which stated that a set of natural numbers S is Diophantine if and only if there exists a polynomial P such that S is precisely the set of natural numbers in the range of P. Using this theorem, along with the above result, there must exist a polynomial P such that a natural number is prime if and only if it is in the positive range of P. See [JSWW] for an explicit construction of such a polynomial; the polynomial in [JSWW] is of degree 25 with 26 variables.

Section 3: Recursive Functions

This section, while not immediately obvious in its relation to the first two, will determine precisely which functions are Diophantine.

Definition: Consider the following functions:

(1)	*Sequence number function*:	$\boldsymbol{S(i,u)}$,
(2)	*The **constant function***:	$\boldsymbol{C(x)=1}$,
(3)	*The **successor function***:	$\boldsymbol{s(x)=x+1}$,
(4)	*The **projection function***:	$\boldsymbol{U_i^n(x_1,\dots,x_n)=x_i}$.

These four functions are referred to as the ***initial functions*** and form the basis of a particular group of functions known as ***recursive functions***. In most definitions, the Sequence Number Function is not defined as an initial function and instead the other three are used to prove it is recursive. It is included here however, for convenience (See Theorem 5.22 of [MF]). Specifically, the set of recursive functions consists of every function that can be obtained through finitely many instances of the initial functions along with the operations of composition, primitive recursion and minimalization (defined below):

Given functions $g_1,\dots,g_m$ and $f(x_1,\dots,x_m)$,
define the **composition** $h=f\circ(g_1,\dots,g_m)$ as follows:

$$\boldsymbol{h(x_1,\dots,x_n)=f\big(g_1(x_1,\dots,x_n),\dots,g_m(x_1,\dots,x_n)\big)}.$$

Given functions f,g such that for all $x_1,\dots,x_n$, there exists y satisfying $(f-g)(x_1,\dots,x_n,y)=0$,
define the **minimalization** of f and g as follows:

$$\boldsymbol{h(x_1,\dots,x_n)=min_y[f(x_1,\dots,x_n,y)=g(x_1,\dots,x_n,y)]}.$$

Given functions $f(x_1,\dots,x_n)$ and $g(t_1,\dots,t_{n+2})$,
define a function $h(x_1,\dots,x_n,z)$ that satisfies the equations of **primitive recursion**:

$$\boldsymbol{h(x_1,\dots,x_n,1)=f(x_1,\dots,x_n)},$$
$$\boldsymbol{h(x_1,\dots,x_n,t+1)=g(t,h(x_1,\dots,x_n,t),x_1,\dots,x_n)}.$$

In computability theory, it turns out that the recursive functions are precisely the set of functions that can computed by ***Turing machines***. This is significant because a function is said to be ***computable*** if there exists an algorithm that can return the output of the function if given an input from the function's domain.

It will now be shown that the set of recursive functions is precisely the set of Diophantine functions. In particular, the Diophantine functions are precisely those that may be computed by a Turing machine.

Theorem 3.1: Let f be a function. Then:

$$\boldsymbol{f}\textbf{ is Diophantine} \leftrightarrow \boldsymbol{f}\textbf{ is recursive.}$$

Proof **(→):** To prove every Diophantine function is recursive, the following lemma is used.

Lemma 3.1.1: Consider the functions: $\boldsymbol{a(x,y) = x + y, b(x,y) = x \cdot y, c_k(x) = k}$
Then $a(x,y)$, $b(x,y)$ and $c_k(x)$ are all recursive functions.

Proof: $\boldsymbol{x + 1 = S(x)}$, $\boldsymbol{x \cdot 1 = U_1^1(x)}$ and $\boldsymbol{c_1(x) = c(x) = 1}$ are trivially recursive. Using composition and primitive recursion, it follows that:

$\boldsymbol{I)}\ \boldsymbol{x + (t + 1) = S(x + t) = S\left(U_2^3(t, x + t, x)\right)}$ $\rightarrow \boldsymbol{a(x,y)}$ is recursive.

$\boldsymbol{II)}\ \boldsymbol{x \cdot (t + 1) = (x \cdot t) + x = U_2^3(t, x \cdot t, x) + U_3^3(t, x \cdot t, x)}$ $\rightarrow \boldsymbol{b(x,y)}$ is recursive.

$\boldsymbol{III)}\ \boldsymbol{c_{k+1}(x) = k + 1 = c_k(x) + c_1(x)}$ $\rightarrow \boldsymbol{c_k(x)}$ is recursive $\forall \boldsymbol{k}$.

It follows from Lemma 3.1.1 that every polynomial with positive integer coefficients is recursive, as they can be expressed through finitely many applications of the functions $a(x,y), b(x,y), c_k(x)$ along with the operation of composition. Suppose f is a Diophantine function, and let P, Q be polynomials with *strictly* nonnegative integer coefficients such that:

$$\boldsymbol{y = f(x_1, \dots, x_n) \leftrightarrow (\exists t_1, \dots, t_m)[(P - Q)(x_1, \dots, x_n, y, t_1, \dots, t_m) = 0]},$$

↓ *(by the Sequence Number Theorem)*

$$\boldsymbol{f(x_1, \dots, x_n) = S\big(1, min_u\big[(P - Q)\big(x_1, \dots, x_n, S(1,u), \dots, S(m+1,u)\big) = 0\big]\big).}$$

By composition and minimalization, f is recursive and every Diophantine function is a recursive function.

Proof **(←):** To prove the converse, clearly the initial functions $c(x), S(x), U_i^n(x_1, \dots, x_n)$ are all Diophantine. By theorem 2.2, $S(i,u)$ is Diophantine. It will be shown that the operations of composition, minimalization and primitive recursion, when applied to Diophantine functions, yield Diophantine functions as well.

Suppose $f, g, g_1, \dots, g_m, r, s$ are Diophantine functions, and define the functions h, k, l:

$$\boldsymbol{h(x_1, \dots, x_n) = f\big(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)\big),}$$
$$\boldsymbol{k(x_1, \dots, x_n) = min_y[r(x_1, \dots, x_n, y) = s(x_1, \dots, x_n, y)],}$$
$$\boldsymbol{l(x_1, \dots, x_n, 1) = f(x_1, \dots, x_n)\ and\ l(x_1, \dots, x_n, t+1) = g(t, l(x_1, \dots, x_n, t), x_1, \dots, x_n).}$$

Then h can be expressed using the following conjunction of Diophantine expressions:

$y = h(x_1, \dots, x_n) \leftrightarrow (\exists t_1, \dots, t_m)\big[\big(t_1 = g_1(x_1, \dots, x_n)\big) \wedge \dots \wedge \big(t_m = g_m(x_1, \dots, x_n)\big) \wedge \big(y = f(t_1, \dots, t_m)\big)\big]$.

Hence, h is Diophantine. Similarly, k can be expressed as the following:

$y = k(x_1, \dots, x_n) \leftrightarrow (\exists z)[z = r(x_1, \dots, x_n, y) = s(x_1, \dots, x_n, y)]^{\wedge}$

$(\forall t)_{\leq y}\big[(t = y) \vee (\exists u, v)\big(u = r(x_1, \dots, x_n, t)\big) \wedge \big(v = s(x_1, \dots, x_n, t)\big) \wedge \big((u < v) \vee (v < u)\big)\big]$.

Therefore, k is also Diophantine. Finally,

$y = l(x_1, \dots, x_n, z) \leftrightarrow (\exists u)\big[(\exists v)\big(v = S(1,u) = f(x_1, \dots, x_n)\big)\big]^{\wedge}$

$(\forall t)_{\leq z}[(t = z) \vee (\exists v)(v = S(t+1, u) = g(t, S(t,u), x_1, \dots, x_n)] \wedge \big(y = S(z,u)\big)$.

Thus, l is Diophantine and so every recursive function is Diophantine as well as vice-versa. ■

One of the more important results in this paper, Theorem 3.1 provides a clear sense of the boundary of Diophantine functions as well as their construction. Moreover, this equivalence carries over to the earlier definition of Diophantine sets given in Section 1.

Definition: A set S of n-tuples of positive integers is called ***recursively enumerable*** if there exists recursive functions $f(x, x_1, \dots, x_n), g(x, x_1, \dots, x_n)$ such that:

$$S = \{(x_1, \dots, x_n) | (\exists x)[f(x, x_1, \dots, x_n) = g(x, x_1, \dots, x_n)]\}.$$

Corollary 3.1.2: Let S be a set.

$$\boldsymbol{S \text{ is Diophantine} \leftrightarrow S \text{ is recursively enumerable.}}$$

Proof: See Theorem 8.1 of [D]. ■

Section 4: Hilbert's Tenth Problem

Using the techniques built across the previous sections, it is finally possible to explicitly construct an enumeration of every Diophantine set of positive integers. Since every polynomial with nonnegative coefficients can be constructed through a series of additions and multiplications from 1 along with a set of variables, suppose the set of variables was fixed in the sequence $x_0, x_1, x_2, \ldots$. Then a sequence of all polynomials with nonnegative coefficients can be defined by the following relation:

$$\boldsymbol{P_1 = 1} \quad \boldsymbol{P_{3i} = P_{L(i)} + P_{R(i)}} \quad \textit{and} \quad \boldsymbol{P_{3i-1} = x_{i-1}} \quad \boldsymbol{P_{3i+1} = P_{L(i)} \cdot P_{R(i)}}$$

Since the functions $L(i)$ and $R(i)$ together traverse all pairs of natural numbers, this construction will systematically introduce every variable as well as list both the sum and product of all previously listed polynomials. For every polynomial, write $P_i = P_i(x_0, \ldots, x_n)$, where n is large enough so that all variables occurring in P_i are included. Then it is possible to construct the following sequence of sets:

$$\boldsymbol{D_n = \{x_0 | (\exists x_1, \ldots, x_n)[P_{L(n)}(x_0, x_1, \ldots, x_n) = P_{R(n)}(x_0, x_1, \ldots, x_n)]\}.}$$

Under this construction, the sequence $D_1, D_2, D_3, D_4, \ldots$ includes all Diophantine sets of natural numbers. To see this, suppose that S is a Diophantine set of natural numbers. From the definition of a Diophantine set, this means that there exists a polynomial P with integer coefficients such that:

$$\boldsymbol{x \in S \leftrightarrow (\exists y_1, \ldots, y_m)[P(x, y_1, \ldots, y_m) = 0]}.$$

The polynomial P can be separated into two polynomials Q_1, Q_2 consisting of all the positive terms in P and of all the negative terms in P, respectively. Then, the equivalence above can be rewritten:

$$\boldsymbol{x \in S \leftrightarrow (\exists y_1, \ldots, y_m)[Q_1(x, y_1, \ldots, y_m) = -Q_2(x, y_1, \ldots, y_m)]}.$$

Note that the terms in Q_2 are all nonpositive, so the polynomial $Q_3 = -Q_2$ consists solely of nonnegative coefficients. Since the sequence of polynomials defined earlier can construct all polynomials with nonnegative coefficients, that means that there exists a and b such that:

$$\boldsymbol{x \in S \leftrightarrow (\exists y_1, \ldots, y_m)[P_a(x, y_1, \ldots, y_m) = P_b(x, y_1, \ldots, y_m)]}.$$

Finally, since the functions $L(i)$ and $R(i)$ traverse all pairs of natural numbers, there exists a natural number n such that $L(n) = a$ and $R(n) = b$. Rewriting the equivalence one last time, it is clear that S is contained in the sequence of Diophantine sets defined earlier, specifically $S = D_n$:

$$\boldsymbol{x \in S \leftrightarrow (\exists y_1, \ldots, y_m)[P_{L(n)}(x, y_1, \ldots, y_m) = P_{R(n)}(x, y_1, \ldots, y_m)]}.$$

It should be noted that this is not a list of all Diophantine sets, since multivariable Diophantine sets such as the *Pythagorean triples* are excluded from this construction. By considering the natural number subscripts of the various D_i, one can consider the set $U = \{(n, x) | x \in D_n\}$. Naturally, one might wonder if the set U is Diophantine.

Theorem 4.1: $\boldsymbol{U = \{(n, x) | x \in D_n\}}$ **is Diophantine.**

Proof: Using the Sequence Number Function, it is claimed that:

$$\boldsymbol{x \in D_n \leftrightarrow (\exists u)\{(S(1,u) = 1) \wedge (S(2,u) = x) \wedge (\forall i)_{\leq n}[S(3i,u) = S(L(i),u) + S(R(i),u)] \wedge (\forall i)_{\leq n}[S(3i+1,u) = S(L(i),u) \cdot S(R(i),u)] \wedge (S(L(n),u) = S(R(n),u)\}}$$

In order to verify this, consider $x \in D_n$ for a given x, n. Then there exists numbers $t_1, \dots, t_n$ such that:

$$\boldsymbol{P_{L(n)}(x, t_1, \dots, t_n) = P_{R(n)}(x, t_1, \dots, t_n).}$$

Choose u such that $\boldsymbol{S(j,u) = P_j(x, t_1, \dots, t_n),\ j = 1, 2, \dots, 3n+2,}$

and so $\boldsymbol{S(2,u) = x}$ and $\boldsymbol{S(3i-1,u) = t_{i-1},\ i = 2, \dots, n+1.}$

It follows that the right side of the equivalence holds. To show the converse, suppose that the right side holds for a given pair of natural numbers x, n. Following the definition of the sequence of all polynomials with nonnegative coefficients provided at the start of the section, one can set $t_1 = S(5, u)$, $t_2 = S(8, u)$ and so on, so that $\boldsymbol{t_i = S(3i+2, u)}$ for $i = 1, \dots, n$. Then $\boldsymbol{S(j,u) = P_j(x, t_1, \dots, t_n)}$ for $j = 1, \dots, 3n+2$. Finally, since $S(L(n), u) = S(R(n), u)$, it must be that:

$$\boldsymbol{P_{L(n)}(x, t_1, \dots, t_n) = P_{R(n)}(x, t_1, \dots, t_n)} \text{ and so } \boldsymbol{x \in D_n}.$$

Thus the above claim holds in both directions and, since the right side is a conjunction of Diophantine expressions, U is a Diophantine set. ■

Although U is Diophantine, using the sequence of Diophantine sets of natural numbers, it is possible to construct a single variable set that is not Diophantine.

Theorem 4.2: $\boldsymbol{V = \{n | n \notin D_n\}}$ **is not Diophantine.**

Proof: Suppose that V is a Diophantine set. Then by the enumeration of the Diophantine sets, $V = D_i$ for some i. However, this is a contradiction as $i \notin D_i \leftrightarrow i \in V \leftrightarrow i \in D_i$. ■

Now that it is understood which functions are computable and therefore Diophantine, as well as how exactly they are related to Diophantine equations and sets, proving there cannot exist an algorithm such as the one described by Hilbert's tenth problem becomes a matter of clever construction.

Specifically, using the set V from Theorem 4.2, it is possible to construct the following function:

Theorem 4.3: $\boldsymbol{g(n,x) = \begin{Bmatrix} 2\ if\ x \in D_n \\ 1\ if\ x \notin D_n \end{Bmatrix}}$ **is not a Diophantine function.**

Proof: Suppose that $g(n,x)$ is a Diophantine function. So there exists some polynomial P such that:

$$\boldsymbol{y = g(n,x) \leftrightarrow (\exists y_1, \dots, y_m)[P(n,x,y,y_1,\dots,y_m) = 0]}.$$

Then by the definition of the set V given in Theorem 4.2, the following equivalence holds:

$$\boldsymbol{x \in V \leftrightarrow (\exists y_1, \dots, y_m)[P(x,x,1,y_1,\dots,y_m) = 0]},$$

and so $$\boldsymbol{V = \{x | (\exists y_1, \dots, y_m)[P(x,x,1,y_1,\dots,y_m) = 0]\}}.$$

This is a contradiction, as it would imply that V is a Diophantine set and this was proven false in the previous theorem.

Therefore, the function $g(n,x) = \begin{Bmatrix} 2\ if\ x \in D_n \\ 1\ if\ x \notin D_n \end{Bmatrix}$ is not Diophantine. ■

The essence of this proof is that if g is a Diophantine function, then V must be a Diophantine set. This is false by Theorem 4.2, however g is constructed as a multivariable function in such a way as to be able to determine the elements of U. Using this, as well as the Diophantine equation corresponding to U, the following theorem demonstrates that if Hilbert's tenth problem was solvable, then $g(n,x)$ would have to be Diophantine.

Theorem 4.4: **Hilbert's tenth problem is unsolvable.**

Proof: Since U is Diophantine, $\boldsymbol{(n,x) \in U \leftrightarrow x \in D_n \leftrightarrow (\exists z_1, \dots, z_k)[P(n,x,z_1,\dots,z_k) = 0]}$.

Suppose there was an algorithm that could determine the existence of integer solutions of Diophantine equations, such as the one described by Hilbert's tenth problem. Then, for a given n and x, this algorithm could be used to determine whether or not the equation $P(n,x,z_1,\dots,z_k) = 0$ defined above has a solution in natural numbers.

From the equivalence, this could determine whether or not $x \in D_n$ and thus allow one to compute the function $g(n,x)$. Since g is not a Diophantine function, it is also not recursive and thus no algorithm should be able to compute g. Therefore, the existence of an algorithm such as the one described by Hilbert's tenth problem is impossible. ■

Thus, there can exist no algorithm that can determine whether a given polynomial with integer coefficients has an integer solution, and so Hilbert's tenth problem is unsolvable.

Section 5: Proving the Exponential Function is Diophantine

Now it is time to prove an assumption made earlier, namely that the *exponential function* $h(n,k) = n^k$, is Diophantine. Historically, this was the last piece of the proof to have been completed so it is apt that it has been saved for the final section. The proof is an extension of the proof that the solutions to the ***Pell Equation***, defined below, are Diophantine.

$$(*)\begin{pmatrix} \boldsymbol{x^2 - dy^2 = 1;\ x,y \geq 0,} \\ \boldsymbol{where\ d = a^2 - 1\ for\ some\ a > 1} \end{pmatrix} \rightarrow \boldsymbol{x^2 - (a^2 - 1)y^2 = 1}.$$

Note the trivial solutions to (*), $(x = 1, y = 0)$ and $(x = a, y = 1)$.

Lemma 5.1: There are no integers x, y satisfying (*) such that $1 < x + y\sqrt{d} < a + \sqrt{d}$.

Proof: Let x, y satisfy (*). Then since $1 = (a + \sqrt{d})(a - \sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d})$, considering the other terms and taking the negative reciprocal of that inequality yields $\boldsymbol{-1 < -x + y\sqrt{d} < -a + \sqrt{d}}$**.** Combining the two inequalities:

$$\boldsymbol{0 < 2y\sqrt{d} < 2\sqrt{d} \rightarrow 0 < y < 1.}$$

Since y is an integer, this is a contradiction. Therefore, no such integers x and y exist. ■

The above lemma states that the two trivial solutions are the "smallest" solutions of a given Pell Equation. Moreover, the following lemma states that any product of two solutions is also a solution of (*).

Lemma 5.2: Let x, y and x', y' be integers which satisfy (*) and define integers x'', y'' by the relation:

$$\boldsymbol{x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d})}.$$

Then x'', y'' satisfy (*).

Proof: Taking the conjugate of the above yields $x'' - y''\sqrt{d} = (x - y\sqrt{d})(x' - y'\sqrt{d})$. Multiplying the two equations together produces the following:

$$\boldsymbol{(x'')^2 - d(y'')^2 = (x^2 - dy^2)((x')^2 - d(y')^2) = 1}.$$

Therefore, x'' and y'' satisfy (*). ■

As a result, the following sequence of solutions to the Pell equation can be constructed:

Definition: Define the sequences $\boldsymbol{x_n(a), y_n(a)}$ for $n \geq 0, a > 1$:

$$\boldsymbol{x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n}.$$

Every x_n, y_n clearly satisfies the Pell equation for a given $a > 1$. The following lemma proves that every solution to the Pell equation is contained within this sequence.

Lemma 5.3: Let x, y be a non-negative solution of (*). Then for some n: $x = x_n, y = y_n$.

Proof: Clearly, $x + y\sqrt{d} \geq 1$. On the other hand, $(a + \sqrt{d})^n$ increases to infinity as n increases.

Hence, for some n: $\boldsymbol{(a + \sqrt{d})^n \leq x + y\sqrt{d} < (a + \sqrt{d})^{n+1}}$.

Suppose there is not equality: $\boldsymbol{(a + \sqrt{d})^n < x + y\sqrt{d} < (a + \sqrt{d})^{n+1}}$.

Since $(x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = 1$, it must be that $x_n - y_n\sqrt{d}$ is positive.

Hence, $1 < (x + y\sqrt{d})(x_n - y_n\sqrt{d}) < a + \sqrt{d}$. This contradicts Lemmas 5.1 and 5.2, and so there must be equality. ■

For the remainder of this section, the notation (x, y) will be used to denote the ***greatest common divisor (g.c.d.)*** of x and y.

Lemma 5.4: $\boldsymbol{(x_n, y_n) = 1}$.

Proof: If $p|x_n$ and $p|y_n$, then $p|(x_n{}^2 - dy_n{}^2) = 1 \rightarrow \boldsymbol{p = 1}$. ■

The following lemmas define an underlying structure for the sequences x_n, y_n using a constant value to represent a in $(*)$. (Refer to Section 2 in [D] for all of the proofs in Lemma 5.5).

Lemma 5.5:

I) $\boldsymbol{x_{m\pm n} = x_m x_n \pm d y_n y_m}$ *and* $\boldsymbol{y_{m\pm n} = x_n y_m \pm x_m y_n}$.

II) $\boldsymbol{x_{m\pm 1} = a x_m \pm d y_m}$ *and* $\boldsymbol{y_{m\pm 1} = a y_m \pm x_m}$.

III) $\boldsymbol{x_{m+1} = 2a x_m - x_{m-1}}$ *and* $\boldsymbol{y_{m+1} = 2a y_m - y_{m-1}}$.

IV) When n is even, y_n is even. When n is odd, y_n is odd.

V) When n is even, x_n is odd.

VI) x_n is increasing. Moreover, $x_{n+1} > x_n \geq a^n$. Finally, $x_n \leq (2a)^n$.

VII) y_n is increasing. Moreover, since $y_0 = 0$, $y_{n+1} > y_n \geq n$. Lastly, $y_n | y_{nk}$.

Lemma 5.6: $\boldsymbol{y_n | y_t \leftrightarrow n | t}$.

Proof: If $n|t$, then it follows from the previous lemma that $y_n|y_t$. Suppose $y_n|y_t$, but $n \nmid t$. Then by the division algorithm, we have: $\boldsymbol{t = nq + r, 0 < r < n}$.

Thus, again by Lemma 5.5: $\boldsymbol{y_t = x_r y_{nq} + x_{nq} y_r}$.

Since $y_n|y_{nq}$ and $(x_{nq}, y_{nq}) = 1$: $\boldsymbol{y_n | x_{nq} y_r \rightarrow y_n | y_r}$.

Since $r < n \rightarrow y_r < y_n$, this is a contradiction and n divides t. ■

The following lemmas demonstrate some of the periodic patterns found within these sequences.

Lemma 5.7: $\boldsymbol{y_{nk} \equiv k x_n^{k-1} y_n \ (mod\ y_n^3).}$

Proof: Consider the equation $x_{nk} + y_{nk}\sqrt{d} = (a + \sqrt{d})^{nk} = (x_n + y_n\sqrt{d})^k$. Expanding the right side of this equation using the binomial theorem yields:

$$\boldsymbol{(x_n + y_n\sqrt{d})^k = \sum_{j=0}^{k} \binom{k}{j} x_n^{k-j}\, y_n^j d^{j/2}.}$$

Thus, $\boldsymbol{y_{nk} = \sum_{\substack{j=1 \\ j\ odd}}^{k} \binom{k}{j} x_n^{k-j}\, y_n^j d^{(j-1)/2} \equiv k x_n^{k-1} y_n + 0 + 0 + \cdots (mod\ y_n^3).}$ ■

Lemma 5.8: $\boldsymbol{y_n \equiv n \ (mod\ (a-1))}$.

Proof: See Lemma 2.14 of [D]. ■

The following three lemmas are particularly abstract and specifically constructed to assist in the final theorems, where it is proved that the *exponential function* is a Diophantine function.

Lemma 5.9: $\boldsymbol{x_n(a) - y_n(a)(a-y) \equiv y^n\ (mod\ 2ay - y^2 - 1)}$.

Proof: Considering the trivial cases where $x = 1, y = 0$ and where $x = a, y = 1$:

$$\boldsymbol{x_0 - y_0(a-y) = 1\ and\ x_1 - y_1(a-y) = y.}$$

The result holds trivially, so one can use Lemma 5.5 and proceed by induction:

$$\boldsymbol{x_{n+1} - y_{n+1}(a-y) = 2a[x_n - y_n(a-y)] - [x_{n-1} - y_{n-1}(a-y)].}$$

Therefore $\boldsymbol{x_{n+1} - y_{n+1}(a-y) \equiv 2ay^n - y^{n-1}\ (mod\ 2ay - y^2 - 1).}$ This completes the proof however, since $\boldsymbol{y^{n-1}(2ay - 1) \equiv y^{n-1}y^2\ (mod\ 2ay - y^2 - 1) = y^{n+1}.}$ ■

Lemma 5.10: If $0 < i \leq n$ and $x_j \equiv x_i\ (mod\ x_n)$, then $\boldsymbol{j \equiv \pm i\ (mod\ 4n)}$.

Proof: See [D], Lemmas 2.20-2.23. ■

Lemma 5.11: $\boldsymbol{{y_n}^2 | y_{ny_n}\ and\ {y_n}^2 | y_t \rightarrow y_n | t.}$

Proof: Setting k to y_n in Lemma 5.7 yields the first result; to get the second, suppose that ${y_n}^2 | y_t$. Then by Lemma 5.6, $t = nk$ for some k.

Since $t = nk$, by Lemma 5.7: $\boldsymbol{y_n^2 | k x_n^{k-1} y_n \rightarrow y_n | k x_n^{k-1}.}$

But $(x_n, y_n) = 1$: $\boldsymbol{y_n | k x_n^{k-1} \rightarrow y_n | k \rightarrow y_n | t.}$ ■

The final lemma demonstrates a relationship between the sequences x_n and y_n when different values are substituted for the variable a in $(*)$.

Lemma 5.12: If $a \equiv b\ (mod\ c)$, then for all n**:**

$$\boldsymbol{x_n(a) \equiv x_n(b),\ y_n(a) \equiv y_n(b)\ (mod\ c)}.$$

Proof: This is clear in the trivial cases, $n = 0, 1$. Proceeding by induction, using Lemma 5.5:

$$\boldsymbol{x_{n+1}(a) = 2ax_n(a) - x_{n-1}(a) \equiv 2bx_n(b) - x_{n-1}(b) = x_{n+1}(b)\ (mod\ c)},$$

and $$\boldsymbol{y_{n+1}(a) = 2ay_n(a) - y_{n-1}(a) \equiv 2by_n(b) - y_{n-1}(b) = y_{n+1}(b)\ (mod\ c)}.$$ ■

Using the lemmas provided, it is now possible to show that the solutions to the Pell Equation can be expressed using a conjunction of Diophantine expressions. Consider the following system of Diophantine equations:

$(\boldsymbol{I})$	$\boldsymbol{x^2 - (a^2 - 1)y^2 = 1}.$
$(\boldsymbol{II})$	$\boldsymbol{u^2 - (a^2 - 1)v^2 = 1}.$
$(\boldsymbol{III})$	$\boldsymbol{s^2 - (b^2 - 1)t^2 = 1}.$
$(\boldsymbol{IV})$	$\boldsymbol{v = ry^2}.$
$(\boldsymbol{V})$	$\boldsymbol{b = 1 + 4py = a + qu}.$
$(\boldsymbol{VI})$	$\boldsymbol{s = x + cu}.$
$(\boldsymbol{VII})$	$\boldsymbol{t = k + 4(d - 1)y}.$
$(\boldsymbol{VIII})$	$\boldsymbol{y = k + e - 1}.$

It will be proven in Theorem 5.13 that this system precisely describes the solutions $x_n(a), y_n(a)$ of a Pell Equation. Following this result, it will be possible to prove (in Theorem 5.14) that the *exponential function* is Diophantine simply by adjoining the following four Diophantine expressions to the above system:

$(\boldsymbol{IX})$	$\boldsymbol{(x - y(a - n) - m)^2 = (f - 1)^2(2an - n^2 - 1)^2}.$
$(\boldsymbol{X})$	$\boldsymbol{m + g = 2an - n^2 - 1}.$
$(\boldsymbol{XI})$	$\boldsymbol{w = n + h = k + l}.$
$(\boldsymbol{XII})$	$\boldsymbol{a^2 - (w^2 - 1)(w - 1)^2z^2 = 1}.$

Theorem 5.13: For given a, x, k, with $a > 1$, the following statement holds:

The Diophantine system $(I - VIII)$ has a solution $\leftrightarrow x = x_k(a)$.

Proof: To prove the left-to-right direction, suppose there exists a solution to the system $(I - VIII)$.

From I, II, III, $\exists\, i, j, n > 0$: $\boldsymbol{x = x_i(a), y = y_i(a),}$

$\boldsymbol{u = x_n(a), v = y_n(a),}$

$\boldsymbol{s = x_j(b), t = y_j(b).}$

From V: $b > a > 1.$

From IV: $\boldsymbol{y \le v \rightarrow i \le n.}$

From V and VI: $\boldsymbol{b \equiv a \ (mod\ x_n(a)), x_j(b) \equiv x_i(a) \ (mod\ x_n(a)).}$

By Lemma 5.12: $\boldsymbol{x_j(b) \equiv x_j(a) (mod\ x_n(a)) \rightarrow x_j(a) \equiv x_i(a) \ (mod\ x_n(a)).}$

Thus, by Lemma 5.10: $\boldsymbol{j \equiv \pm i \ (mod\ 4n).}$

By Lemma 5.11, since $y^2 | y_n$, $y | n$: $\boldsymbol{j \equiv \pm i \ (mod\ 4y_i(a)).}$ **(1)**

From V: $\boldsymbol{b \equiv 1 \ (mod\ 4y_i(a)) \rightarrow b - 1 \equiv 0 \ (mod\ 4y_i(a)).}$

By Lemma 5.8 and VII: $\boldsymbol{y_j(b) \equiv j \ (mod\ 4y_i(a)) \equiv k \ (mod\ 4y_i(a)).}$ **(2)**

Combining (1) and (2) yields: $\boldsymbol{k \equiv \pm i \ (mod\ 4y_i(a)).}$

Since $i, k \le y_i(a)$ and the numbers $-2y + 1, -2y + 2, -2y + 3, \dots, -1, 0, 1, \dots, 2y$ all form a complete set of mutually incongruent residues modulo $4y = 4y_i(a)$, this implies that $\boldsymbol{k = i}$. Therefore, substituting into the definition of x yields $\boldsymbol{x = x_i(a) = x_k(a)}$.

Conversely, let $\boldsymbol{x = x_k(a)}$ and $\boldsymbol{y = y_k(a)}$. $\rightarrow I$ is satisfied.

Let $m = 2ky_k(a)$ and set: $\boldsymbol{u = x_m(a)\ and\ v = y_m(a).}$ $\rightarrow II$ is satisfied.

By Lemmas 5.6 and 5.11: $\boldsymbol{y_k^2 | y_{ky_k}\ and\ y_{ky_k} | y_{2ky_k} \rightarrow y^2 | v.}$ $\rightarrow IV$ is satisfied.

Then by lemma 5.5, since m is even, it must be that $x_m(a) = u$ is odd and so $(u, 4vy) = 1$. By the *Chinese Remainder Theorem*: $\exists b_0$ such that $\boldsymbol{b_0 \equiv 1\ (mod\ 4y)}$, $\boldsymbol{b_0 \equiv a\ (mod\ u)}$. Since every natural number of the form $b_0 + 4juy$ satisfies these congruences, where j is a natural number, there must exist b, p, q such that: $\boldsymbol{b = 1 + 4py = a + qu.}$ $\rightarrow V$ is satisfied.

Now, define $\boldsymbol{s = x_k(b)}$ and $\boldsymbol{t = y_k(b)}$. Since $b > a$, it must be that $s > x$. $\rightarrow III$ is satisfied.

By Lemma 5.12, as well as V: $\boldsymbol{b \equiv a\ (mod\ u) \rightarrow s \equiv x\ (mod\ u).}$ $\rightarrow VI$ is satisfied.

By Lemmas 5.5 and 5.8: $\boldsymbol{t \ge k, t \equiv k \ (mod\ (b - 1)) \rightarrow t \equiv k\ (mod\ 4y).}$ $\rightarrow VII$ is satisfied.

Finally, by lemma 5.5: $\boldsymbol{y \ge k.}$ $\rightarrow VIII$ is satisfied. ■

Following Theorem 5.13, there are only a couple small results that will be needed in order to prove that the conjunction of the twelve expressions precisely describes the exponential function.

Corollary 5.13.1: The function $g(z,k) = x_k(z+1)$ is Diophantine.

Lemma 5.13.2: If $a > y^k$, then $2ay - y^2 - 1 > y^k$.

Proof: Set $\boldsymbol{g(y) = 2ay - y^2 - 1}$**.** Then, since it must be that $a \geq 2$, clearly $\boldsymbol{g(1) = 2a - 2 \geq a}$**.**

For $1 \leq y < a$: $\boldsymbol{g'(y) = 2a - 2y > 0 \rightarrow g(y) \geq a}$.

Thus, for $a > y^k \geq y$: $\boldsymbol{2ay - y^2 - 1 \geq a > y^k}$. ■

Finally it can be shown that the exponential function is Diophantine, completing the gap in the proof, affirming the proof that the factorial function is Diophantine and so on.

Theorem 5.14: $\boldsymbol{m = n^k \leftrightarrow}$ **The Diophantine system** $\boldsymbol{(I - XII)}$ **has a solution.**

Proof: Suppose the system $(I - XII)$ holds. From XI, it must be that $w > 1$. Plugging this value into XII, it can be seen that: $\boldsymbol{(w-1)z > 0 \rightarrow a^2 > 1 \rightarrow a > 1}$.

Since $a > 1$, it is possible to use Theorem 5.13 and so $\boldsymbol{x = x_k(a), y = y_k(a)}$.

Then, by Lemma 5.9 and IX: $\boldsymbol{m \equiv n^k \ (mod\ 2an - n^2 - 1)}$.

By XI: $\boldsymbol{k, n < w}$.

Then, by Lemma 5.3 and XII: $\exists \boldsymbol{j}$ such that $\boldsymbol{a = x_j(w), (w-1)z = y_j(w)}$.

By Lemma 5.8: $\boldsymbol{(w-1)z \equiv j \ \big(mod\ (w-1)\big) \rightarrow j \equiv 0 \ \big(mod\ (w-1)\big)}$.

So $\boldsymbol{j \geq w - 1}$, and by Lemma 5.5: $\boldsymbol{a \geq w^{w-1} > n^k}$.

Finally, by Lemma 5.13.2 and X: $\boldsymbol{m, n^k < 2an - n^2 - 1 \rightarrow m = n^k}$.

Proof $(\rightarrow)$: Conversely, suppose that $\boldsymbol{m = n^k}$. One can choose any number w such that $w > n, k$ and set $\boldsymbol{a = x_{w-1}(w) > 1}$. Then by Lemma 5.8:

$$\boldsymbol{y_{w-1}(w) \equiv 0 \ \big(mod\ (w-1)\big)}.$$

Thus: $\boldsymbol{y_{w-1}(w) = z(w-1)}$. $\rightarrow XII$ is satisfied.

By setting $h = w - n$ and $l = w - k$: $\rightarrow XI$ is satisfied.

By Lemma 5.5, it must be that $a \geq w^{w-1} > n^k$. So Lemma 5.13.2 can again be used to show that:

$$\boldsymbol{m = n^k < 2an - n^2 - 1}. \qquad \rightarrow X \text{ is satisfied.}$$

Finally, one can set $x = x_k(a)$ and $y = y_k(a)$ and use Lemma 5.9 to define f as the following:

$$\boldsymbol{x - y(a - n) - m = \pm(f - 1)(2an - n^2 - 1)}. \qquad \rightarrow IX \text{ is satisfied.}$$

It follows from Theorem 5.13 that $I - VIII$ is satisfied. ■

Section 6: Bibliography

[D] Martin Davis, *Hilbert's tenth problem is unsolvable,* Amer. Math. Monthly **80** (1973), 233-269.

[H] Sir Thomas Little Heath, *Diophantus of Alexandria: A Study in the History of Greek Algebra*, University Press, Cambridge, MA, 1910.

[JSWW] James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens, *Diophantine representation of the set of prime numbers*, Amer. Math. Monthly **83** (1976), no. 6, 449-464.

[Ma] Yuri Matiyasevich, *Hilbert's tenth problem*, MIT Press, Cambridge, MA, 1993.

[MF] M. Ram Murty and Brandon Fodden, *Hilbert's tenth problem. An introduction to logic, number theory, and computability*. Student Mathematical Library, 88. American Mathematical Society, Providnce, RI, 2019.