# Hilbert's Tenth Problem: Undecidability of Polynomial Equations

Alexandra Shlapentokh

Department of Mathematics,
East Carolina University,
Greenville, North Carolina, USA

June 20, 2008

# Table of Contents

# Hilbert's Question about Polynomial Equations

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers?

Using modern terms one can ask if there exists a program taking coefficients of a polynomial equation as input and producing "yes" or "no" answer to the question "Are there integer solutions?".

This problem became known as Hilbert's Tenth Problem

# The Answer

This question was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matiyasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine subsets of $\mathbb{Z}$.

# Recursive and Recursively Enumerable Subsets of $\mathbb{Z}$

## Recursive Sets

A set $A \subseteq \mathbb{Z}^m$ is called recursive or decidable if there is an algorithm (or a computer program) to determine the membership in the set.

## Recursively Enumerable Sets

A set $A \subseteq \mathbb{Z}^m$ is called recursively enumerable if there is an algorithm (or a computer program) to list the set.

## Theorem

*There exist recursively enumerable sets which are not recursive.*

## Diophantine Sets

A subset $A \subset \mathbb{Z}^m$ is called Diophantine over $\mathbb{Z}$ if there exists a polynomial $p(T_1, \ldots T_m, X_1, \ldots, X_k)$ with rational integer coefficients such that for any element $(t_1, \ldots, t_m) \in \mathbb{Z}^m$ we have that

$$\exists x_1, \ldots, x_k \in \mathbb{Z} : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of $A$ over $\mathbb{Z}$.

## Corollary

*There are undecidable Diophantine subsets of $\mathbb{Z}$.*

# Existence of Undecidable Diophantine Sets Implies No Algorithm

Suppose $A \subset \mathbb{Z}$ is an undecidable Diophantine set with a Diophantine definition $P(T, X_1, \ldots, X_k)$. Assume also that we have an algorithm to determine existence of integer solutions for polynomials. Now, let $a \in \mathbb{Z}_{>0}$ and observe that $a \in A$ iff $P(a, X_1, \ldots, X_K) = 0$ has solutions in $\mathbb{Z}^k$. So if can answer Hilbert's question effectively, we can determine the membership in $A$ effectively.

# Diophantine Sets Are Recursively Enumerable

It is not hard to see that Diophantine sets are recursively enumerable. Given a polynomial $p(T, \bar{X})$ we can effectively list all $t \in \mathbb{Z}$ such that $p(t, \bar{X}) = 0$ has a solution $\bar{x} \in \mathbb{Z}^k$ in the following fashion. Using a recursive listing of $\mathbb{Z}^{k+1}$, we can plug each $(k+1)$-tuple into $p(T, \bar{X})$ to see if the value is 0. Each time we get a zero we add the first element of the $(k+1)$-tuple to the $t$-list.

# A Simple Example of a Diophantine Set over $\mathbb{Z}$

**The set of even integers**

$$\{t \in \mathbb{Z} | \exists w \in \mathbb{Z} : t = 2w\}$$

To construct more complicated examples we need to establish some properties of Diophantine sets.

# Intersections and Unions of Diophantine Sets

**Lemma**

*Intersections and unions of Diophantine sets are Diophantine.*

**Proof.**

Suppose $P_1(T, \bar{X}), P_2(T, \bar{Y})$ are Diophantine definitions of subsets $A_1$ and $A_2$ of $\mathbb{Z}$ respectively over $\mathbb{Z}$. Then

$$P_1(T, \bar{X})P_2(T, \bar{Y})$$

is a Diophantine definition of $A_1 \cup A_2$, and

$$P_1^2(T, \bar{X}) + P_2^2(T, \bar{Y})$$

is a Diophantine definition of $A_1 \cap A_2$. □

# One vs. Finitely Many

**Lemma (Replacing Finitely Many by One)**

*Any finite system of equations over $\mathbb{Z}$ can be effectively replaced by a single polynomial equation over $\mathbb{Z}$ with the identical $\mathbb{Z}$-solution set.*

# One vs. Finitely Many

**Proof.**

Consider a system of equations

$$\begin{cases} g_1(x_1, \ldots, x_k) = 0 \\ g_2(x_1, \ldots, x_k) = 0 \\ \qquad \ldots \\ g_m(x_1, \ldots, x_k) = 0 \end{cases}$$

This system has solutions in $\mathbb{Z}$ if and only if the following equation has solutions in $\mathbb{Z}$:

$$g_1(x_1, \ldots, x_k)^2 + g_2(x_1, \ldots, x_k)^2 + \ldots + g_m(x_1, \ldots, x_k)^2 = 0$$

# One vs. Finitely Many

**Corollary**

*We can let the Diophantine definitions consist of several polynomials without changing the nature of the relation.*

# A Tool for Diophantine Definitions: Write GCD as a Linear Combination

**Proposition**

*Let $a, b \in \mathbb{Z}_{\neq 0}$ with $(a, b) = 1$. The there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

# More Complicated Diophantine Definitions

**Proposition**

*The set of non-zero integers has the following Diophantine definition:*

$$\{t \in \mathbb{Z} | \exists x, u, v \in \mathbb{Z} : (2u-1)(3v-1) = tx\}$$

**Proof.**

If $t = 0$, then either $2u - 1 = 0$ or $3v - 1 = 0$ has a solution in $\mathbb{Z}$, which is impossible.
Suppose now $t \neq 0$. Write $t = t_2 t_3$, where $t_2$ is odd and $t_3 \not\equiv 0 \mod 3$. Then since $(t_2, 2) = 1$ and $(t_3, 3) = 1$, by a property of GCD there exist $u, x_u, v, x_v \in \mathbb{Z}$ such that $2u + t_2 x_u = 1$ and $3v + t_3 x_v = 1$. Then $(2u-1)(3v-1) = t_2 x_u t_3 x_v = t(x_u x_v)$. □

## The set of non-negative integers

From Lagrange's Theorem we get the following representation of non-negative integers:

$$\{t \in \mathbb{Z} | \exists x_1, x_2, x_3, x_4 : t = x_1^2 + x_2^2 + x_3^2 + x_4^2\}$$

# A General Question

**A Question about an Arbitrary Recursive Ring $R$**

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in $R$, can determine whether this equation has solutions in $R$?

**The most prominent open questions are probably the decidability of HTP for $R = \mathbb{Q}$ and $R$ equal to the ring of integers of an arbitrary number field.**

# Undecidability of HTP over $\mathbb{Q}$ Implies Undecidability of HTP for $\mathbb{Z}$

Indeed, suppose we knew how to determine whether solutions exist over $\mathbb{Z}$. Let $Q(x_1, \ldots, x_k)$ be a polynomial with rational coefficients. Then

$$\exists x_1, \ldots, x_k \in \mathbb{Q} : Q(x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$\exists y_1, \ldots, y_k, z_1, \ldots, z_k \in \mathbb{Z} : Q(\frac{y_1}{z_1}, \ldots, \frac{y_k}{z_k}) = 0 \wedge z_1 \ldots z_k \neq 0.$$

So decidability of HTP over $\mathbb{Z}$ would imply the decidability of HTP over $\mathbb{Q}$.

# Using Diophantine Definitions to Solve the Problem

**Lemma**

*Let $R$ be a recursive ring containing $\mathbb{Z}$ and such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over $R$. Then HTP is not decidable over $R$.*

**Proof.**

Let $h(T_1, \ldots, T_l)$ be a polynomial with rational integer coefficients and consider the following system of equations.

$$\begin{cases} h(T_1, \ldots, T_l) = 0 \\ p(T_1, \bar{X}_1) = 0 \\ \cdots \\ p(T_l, \bar{X}_l) = 0 \end{cases} \tag{1}$$

It is easy to see that $h(T_1, \ldots, T_l) = 0$ has solutions in $\mathbb{Z}$ iff (1) has solutions in $R$. Thus if HTP is decidable over $R$, it is decidable over $\mathbb{Z}$. □

# The Plan

So to show that HTP is undecidable over $\mathbb{Q}$ we just need to construct a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$!!!

# A Conjecture of Barry Mazur

## The Conjecture on the Topology of Rational Points

Let $V$ be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

## A Nasty Consequence

There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

Actually if the conjecture is true, no infinite and discrete (in the archimedean topology) set has a Diophantine definition over $\mathbb{Q}$.

# Understanding Mazur's Conjecture

Suppose you are given a system of polynomial equations:

$$\begin{cases} P_1(x_1, \ldots, x_k) = 0 \\ P_2(x_1, \ldots, x_k) = 0 \\ \qquad \ldots \\ P_m(x_1, \ldots, x_k) = 0 \end{cases} \tag{2}$$

Think of solutions to this system as points in $\mathbb{R}^k$ but consider only the points whose coordinates are rational numbers. In other words we are interested in the set

$$RP = \{(x_1, \ldots, x_k) \in \mathbb{Q}^k : (x_1, \ldots, x_k) \text{ is a solution to system (2)}\}.$$

Now take the topological closure of $RP$ in $\mathbb{R}^k$ (i.e. the points plus the "boundary"). Mazur's conjecture asserts that the resulting set will have finitely many "connected pieces".

# Another Plan: Diophantine Models

## What is a Diophantine Model of $\mathbb{Z}$?

Let $R$ be a recursive ring whose fraction field is not algebraically closed and let $\phi : \mathbb{Z} \longrightarrow R^k$ be a recursive injection mapping Diophantine sets of $\mathbb{Z}$ to Diophantine sets of $R^k$. Then $\phi$ is called a Diophantine model of $\mathbb{Z}$ over $R$.

# Another Plan: Diophantine Models

## Sending Diophantine Sets to Diophantine Sets Makes the Map Recursive

Actually the recursiveness of the map will follow from the fact that the $\phi$-image of the graph of addition is Diophantine. Indeed, if the $\phi$-image of the graph of addition is Diophantine, it is recursively enumerable. So we have an effective listing of the set

$$D_+ = \{(\phi(m), \phi(n), \phi(m+n)), m, n \in \mathbb{Z}\}.$$

Assume we have computed $\phi(k-1)$. Now start listing $D_+$ until we come across a triple whose first two entries are $\phi(k-1)$ and $\phi(1)$. Then third element of the triple must be $\phi(k)$.

## Making Addition and Multiplication Diophantine is Enough

It is enough to require that the $\phi$-images of the graphs of $\mathbb{Z}$-addition and $\mathbb{Z}$-multiplication are Diophantine over $R$. For example, consider the $\phi$ image of a set

$$D = \{t \in \mathbb{Z} | \exists x \in \mathbb{Z} : t = x^2 + x\}$$

Let $D_\times$ be the graph of multiplication and let $D_+$ be the graph of addition. Then by assumption $\phi(D_\times)$ and $\phi(D_+)$ are Diophantine sets with $R$-Diophantine definitions $F_+(A, B, C, \bar{Y})$ and $F_x(A, B, C, \bar{Z})$ respectively. Thus, we have that $T \in \phi(D)$ iff $\exists W, X \in R$ such that $(W, X, T) \in \phi(D_+)$ (i.e. $T = \phi(t), X = \phi(x), W = \phi(w), t = x + w$) and $(X, X, W) \in \phi(D_\times)$ (i.e. $w = x^2$). Using Diophantine definitions we can rephrase this in the following manner: $T \in \phi(D)$ iff there exist $W, X, \bar{Y}, \bar{Z}$ in $R$ such that

$$\begin{cases} F_+(W, X, T, \bar{Y}) = 0 \text{ ( i.e. } (W, X, T) \in \phi(D_+)) \\ F_\times(X, X, W, \bar{Z}) = 0 \text{ ( i.e. } (X, X, W) \in \phi(D_\times)) \end{cases}$$

## Diophantine Model of $\mathbb{Z}$ Implies Undecidability

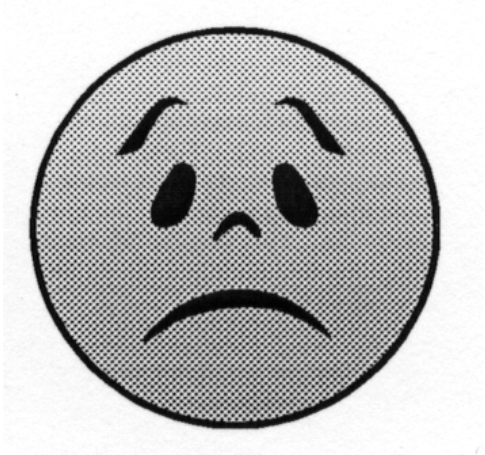
If $R$ has a Diophantine model of $\mathbb{Z}$, then $R$ has undecidable Diophantine sets. Indeed, let $A \subset \mathbb{Z}$ be an undecidable Diophantine set. Suppose we want to determine whether an integer $n \in A$. Instead of answering this question directly we can ask whether $\phi(n) \in \phi(A)$. By assumption $\phi(n)$ is algorithmically computable. So if $\phi(A)$ is a computable subset of $R$, we have a contradiction.

## So all we need is a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$!!!!

# A Theorem of Cornelissen and Zahidi

**Theorem**

*If Mazur's conjecture on topology of rational points holds, then there is no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.*



# The Rings between $\mathbb{Z}$ and $\mathbb{Q}$

## A Ring in between

Let $\mathcal{S}$ be a set of primes of $\mathbb{Q}$. Let $O_{\mathbb{Q},\mathcal{S}}$ be the following subring of $\mathbb{Q}$.

$$\left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, n \text{ is divisible by primes of } \mathcal{S} \text{ only} \right\}$$

If $\mathcal{S} = \emptyset$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Z}$. If $\mathcal{S}$ contains all the primes of $\mathbb{Q}$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Q}$. If $\mathcal{S}$ is finite, we call the ring small. If $\mathcal{S}$ is infinite, we call the ring large.

## Example of a Small Ring not Equal to $\mathbb{Z}$

$$\{ \frac{m}{3^a 5^b} : m \in \mathbb{Z}, a, b \in \mathbb{Z}_{>0} \}$$

## Example of a Big Ring not Equal to $\mathbb{Q}$

$$\{\frac{m}{\prod p_i^{n_i}} : p_i \equiv 1 \mod 4, n_i \in \mathbb{Z}_{>0}\}$$

## Remark

Observe that $\mathbb{Q}$ is the fraction field of any small or big ring.

# Diophantine Properties of Big and Small Rings

**Lemma**

*The set of non-zero elements of a big or a small ring is Diophantine over the ring.*

**Corollary**

*Let $R$ be a big or a small ring. Let $A \subset \mathbb{Q}^m$ be Diophantine over $\mathbb{Q}$. Then $A \cap R^m$ is Diophantine over $R$.*

# Diophantine Properties of Big and Small Rings

**Proof.**

Let $f(T_1, \ldots, T_m, X_1, \ldots, X_K)$ be a Diophantine definition of $A$ over $\mathbb{Q}$. In other words, $\forall t_1, \ldots, t_m \in \mathbb{Q}$, we have that

$$(t_1, \ldots, t_m) \in A \iff \exists x_1, \ldots, x_k \in \mathbb{Q} : f(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

Now we are going to replace each $t_i$ by $\frac{u_i}{v_i}$ with $u_i, v_i \in R$ and $v_i \neq 0$ to obtain the following: $t_1, \ldots, t_m \in A \cap R \iff$

$$\exists u_1, v_1 \ldots, u_k, v_k \in R : f(t_1, \ldots, t_m, \frac{u_1}{v_1}, \ldots, \frac{u_k}{v_k}) = 0 \wedge \prod_{i=1}^{k} v_i \neq 0$$

$$\Updownarrow$$

$$\exists u_1, v_1 \ldots, u_k, v_k \in R :$$

$$(\prod_{i=1}^{k} v_i)^{\deg(f)} f(t_1, \ldots, t_m, \frac{u_1}{v_1}, \ldots, \frac{u_k}{v_k}) = 0 \wedge \prod_{i=1}^{k} v_i \neq 0$$

# Diophantine Properties of Big and Small Rings

## Proposition

1. *"One=finitely many" over big and small rings.*
2. *The set of non-negative elements of a big or a small ring $R$ is Diophantine over $R$: a small modification of the Lagrange argument is required to accomodate possible denominators*

$$\{t \in R | \exists x_1, x_2, x_3, x_4, x_5 : x_5^2 t = x_1^2 + x_2^2 + x_3^2 + x_4^2 \wedge x_5 \neq 0\}$$

# Order at a Prime

## Definition

Let $p$ be a prime number. Let $x \neq 0$ be an integer. Let $n \in \mathbb{Z}_{\geq 0}$ be such that $p^n$ divides $x$ but $p^{n+1}$ does not divide $x$. Then let $\text{ord}_p\, x = n$. If $y \in \mathbb{Q}, y \neq 0$ and $y = \frac{x_1}{x_2}$, where $x_1, x_2 \in \mathbb{Z}_{\neq 0}$, then let $\text{ord}_p\, y = \text{ord}_p\, x_1 - \text{ord}_p\, x_2$. Also let $\text{ord}_p\, 0 = \infty$. If $x \in \mathbb{Q}$ and $ord_p x \geq 0$ we say that $x$ is integral at $p$.

## Example

$\text{ord}_3(\frac{25}{9}) = -2, \text{ord}_5(\frac{25}{9}) = 2, \text{ord}_7(\frac{25}{9}) = 0$

# Some Properties of Order

**Lemma**

- *If* $x, y \in \mathbb{Q}$, $p$ *– a prime of* $\mathbb{Q}$ *and* $\operatorname{ord}_p x < \operatorname{ord}_p y$, *then* $\operatorname{ord}_p(x + y) = \operatorname{ord}_p x$.
- $\operatorname{ord}_p x^n = n \operatorname{ord}_p x$ *for any* $n \in \mathbb{Z}$.

**Example**

$ord_5(25 + 125) = \operatorname{ord}_5 25 = 2 = \operatorname{ord}_5 150$

# Another Way to Look at Big and Small Rings

Let $\mathcal{S}$ be a set of primes. Then a ring

$$O_{\mathbb{Q},\mathcal{S}} = \{x \in \mathbb{Q} : \mathrm{ord}_p\, x \geq 0 \ \forall p \notin \mathcal{S}\}$$

is called a small ring if $\mathcal{S}$ is finite and big otherwise.

# Defining Order is Enough

**Theorem**

*Suppose the set of rational numbers integral at any given prime is Diophantine over $\mathbb{Q}$. Then $\mathbb{Z}$ is Diophantine over any small ring.*

**Proof.**

Let $\mathcal{S} = \{p_1, \ldots, p_k\}$. Note that for any prime $p$, the set of elements of $O_{\mathbb{Q},\mathcal{S}}$ integral at $p$ is Diophantine over $O_{\mathbb{Q},\mathcal{S}}$. This is a consequence of the fact that we can define the set of non-zero elements of $O_{\mathbb{Q},\mathcal{S}}$ (see Frame 8.) Putting several Diophantine definitions together we conclude that the set of elements of $O_{\mathbb{Q},\mathcal{S}}$ integral at $p_1, \ldots, p_k$ is Diophantine over $O_{\mathbb{Q},\mathcal{S}}$. However, integers are precisely the elements of $O_{\mathbb{Q},\mathcal{S}}$ integral at all the primes of $\mathcal{S}$. □

# Defining Integers over Small Subrings of $\mathbb{Q}$

**Theorem (Julia Robinson)**

*$\mathbb{Z}$ has a Diophantine definition over any small subring of $\mathbb{Q}$.*

# Some Ideas behind the Proof

## Claim

Let $x \in \mathbb{Q}$, let $p$ be a prime number. Then $\operatorname{ord}_p(\frac{x^2}{p} + \frac{1}{p^2})$ is even if and only if $\operatorname{ord}_p x \geq 0$.

## Proof.

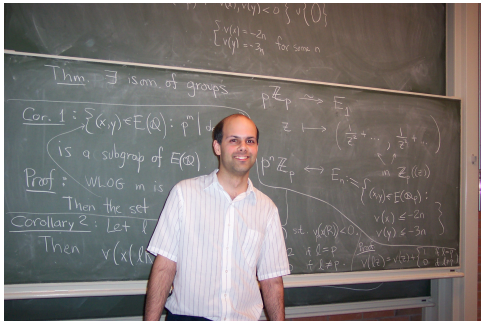
Suppose $\operatorname{ord}_p x < 0$. Then
$\operatorname{ord}_p \frac{x^2}{p} = 2 \operatorname{ord}_p x - 1 \leq -3 < \operatorname{ord}_p \frac{1}{p^2} = -2$. Thus,
$\operatorname{ord}_p(\frac{x^2}{p} + \frac{1}{p^2}) = \operatorname{ord}_p \frac{x^2}{p} = 2 \operatorname{ord}_p x - \operatorname{ord}_p p = 2 \operatorname{ord}_p x - 1 \not\equiv 0 \mod 2$.
Suppose now that $\operatorname{ord}_p x \geq 0$. Then $\operatorname{ord}_p \frac{x^2}{p} \geq -1$. Therefore
$\operatorname{ord}_p \frac{x^2}{p} > \operatorname{ord}_p \frac{1}{p^2} = -2$ and $\operatorname{ord}_p(\frac{x^2}{p} + \frac{1}{p^2}) = \operatorname{ord}_p \frac{1}{p^2} = -2 \equiv 0 \mod 2$ □

# Some Ideas behind the Proof

## Another Step in the Proof

Let $p$ be a prime number such that 5 is not a square modulo $p$. (For example we can let $p = 3$.) Then $a^2 - 5b^2 = z$ has solutions in $\mathbb{Z}$ only if $\operatorname{ord}_p z$ is even.

# The Statement of Poonen's Theorem




**Theorem**

*There exist recursive sets of primes $\mathcal{T}_1$ and $\mathcal{T}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of primes containing $\mathcal{T}_1$ and avoiding $\mathcal{T}_2$, the following hold:*

- *$\mathbb{Z}$ has a Diophantine model over $O_{\mathbb{Q},\mathcal{S}}$.*
- *Hilbert's Tenth Problem is undecidable over $O_{\mathbb{Q},\mathcal{S}}$.*

# What is Natural Density?

## Definition

Let $\mathcal{A}$ be a set of primes. Then the natural density of $\mathcal{A}$ is equal to the limit below (if it exists):

$$\lim_{X \to \infty} \frac{\#\{p \in A, p \leq X\}}{\#\{p \leq X\}}$$

# A Proof Overview

We start with an equation of the form

$$y^2 = x^3 + ax + b.$$

with $4a^3 + 27b^2 \neq 0$. We can choose $a, b \in \mathbb{Z}$ and a set of primes $\mathcal{S}$ so that in $O_{\mathbb{Q},\mathcal{S}}$ all the solutions $(x, y)$ to this equation with $y > 0$ constitute the set

$$\{(x_i, y_i)\} \cup \{ \text{ finite set of pairs } \},$$

where $|y_j - j| < 10^{-j}$. Note that we know how to define positive numbers using a variation on Lagrange's theme (see Frame 10) and how to get rid of a finite set of undesirable values (just say "$\neq$" as in Frame 8).

# Constructing a Model of $\mathbb{Z}_{>0}$ using $y_j$'s

We claim that $\phi : j \longrightarrow y_j$ is a Diophantine model of $\mathbb{Z}_{>0}$. In other words we claim that $\phi$ is a recursive injection and the following sets are Diophantine:

$$D+ = \{(y_i, y_j, y_k) \in D^3 : k = i + j, k, i, j \in \mathbb{Z}_{>0}\}$$

and

$$D_2 = \{(y_i, y_k) \in D^2 : k = i^2, i \in \mathbb{Z}_{>0}\}.$$

(Note that if $D+$ and $D_2$ are Diophantine, then $D_\times = \{(y_i, y_j, y_k) \in D^3 : k = ij, k, i, j \in \mathbb{Z}_{>0}\}$ is also Diophantine since $xy = \frac{1}{2}((x + y)^2 - x^2 - y^2.)$

# Constructing a Model of $\mathbb{Z}_{>0}$ Using $y_j$

## Sums and Squares Are Diophantine

It is easy to show that

$$k = i + j \Leftrightarrow |y_i + y_j - y_k| < 1/3.$$

and with the help of Lagrange this makes $D_+$ Diophantine. Similarly we have that

$$k = i^2 \Leftrightarrow |y_i^2 - y_k| < 2/5,$$

implying that $D_2$ is Diophantine.