Julia Robinson and Hilbert's Tenth Problem*

Jaikumar Radhakrishnan and S P Suresh

Hilbert's Tenth Problem asks whether there is an algorithmic procedure to solve Diophantine equations (polynomial equations with integer coefficients) for integer solutions. This famous problem was shown to be *unsolvable* by Yuri Matiyasevič in 1970. In other words, there is no algorithm that can *decide* in general whether a given Diophantine equations has integer solutions or not. This negative solution builds on a long line of work by Martin Davis, Hilary Putnam, and importantly, Julia Robinson. In this article, we briefly describe the problem, its unsolvability, and Julia Robinson's contribution.

Jaikumar Radhakrishnan is a theoretical computer scientist currently working as a distinguished professor at the International Centre for Theoretical Sciences (ICTS-TIFR), Bengaluru.

S P Suresh is a theoretical computer scientist currently working as a professor at the Chennai Mathematical Institute (CMI), Kelambakkam.

Keywords
Diophantine equations, Hilbert's tenth problem, effective procedures, algorithmic unsolvability.

1. Julia Robinson – A Brief Biography

When Julia Robinson passed away at the age of 65 on 30 July 1985, the American Mathematical Society lost a former president (1981–82), the US National Academy of Sciences lost the first woman mathematician it elected as a member, and the world, a most remarkable figure of 20th century mathematics. Indeed, Julia Robinson's mathematics reflected the ideas that sprouted in the 20th century – what could a computer not do? When she reached the University of California, Berkeley, she learnt number theory from Raphael M Robinson (whom she later married in 1941). He suggested to her a problem on recursive functions which she solved and published. She audited a seminar on Gödel's results given by Alfred Tarski, under whose supervision she obtained a PhD in 1948 for her thesis "Definability and decision problems in arithmetic". Soon after her PhD, she began working on Hilbert's tenth problem: *is there an effective method for determining if a given Diophantine equation has a solution in*

*Vol.29, No.6, DOI: https://doi.org/10.1007/s12045-024-0747-4

For the next almost two decades, working along with Martin Davis, Hilary Putnam, and others, she made several contributions to this subject, including an influential hypothesis on the growth of Diophantine relations, which came to be called Robinson's Hypothesis.

integers. For the next almost two decades, working along with Martin Davis, Hilary Putnam, and others, she made several contributions to this subject, including an influential hypothesis on the growth of Diophantine relations, which came to be called Robinson's Hypothesis. She was delighted when in 1970 a young Russian mathematician Yuri Matiyasevič showed that the Fibonacci numbers satsify the hypothesis, and, therefore, that the answer to Hilbert's tenth problem is *negative*. A week after learning about this breakthrough, she wrote to Matiyasevič [1]:

> *. . . now I know it is true, it is beautiful, it is wonderful.*
> *If you really are 22, I am especially pleased to think that when I first made the conjecture you were a baby and I just had to wait for you to grow up!*

That the Tenth Problem should be solved in her lifetime was for her a longstanding wish: "I felt that I couldn't bear to die without knowing the answer".

That the Tenth Problem should be solved in her lifetime was for her a longstanding wish: "I felt that I couldn't bear to die without knowing the answer" [1]. As a child, Julia had wished for a bicycle, which she eventually got. Her life and her lifetime were not simple, and even these straightforward wishes at different times seemed likely to remain unfulfilled.

When Julia Bowman was born on 8 December 1919, her parents with her elder sister, Constance, lived in St. Louis, Missouri. Julia's mother passed away when Julia was two. Her father sent the sisters along with a nurse to live with their grandmother in Arizona. Their father remarried and moved to Arizona himself. For the girls' education, the family moved to a place near San Diego, where a third sister, Billie, joined them in 1928. Scarlet fever and rheumatic fever struck Julia in succession, and she spent a year in bed. She feared that she would never get the bicycle that her father promised to buy her once she recovered. To make up for the lost time in her education, the family employed a retired teacher as a tutor, and in just one year Julia mastered four years' worth of school material. When she returned to school, she found herself isolated, and till the end had but one friend. She was taught mathematics by women teachers (her tutor was also a woman), and towards the end of school she was the only girl in a room full of boys taking mathematics. She excelled in mathematics and physics. The Great Depression had set in when she had returned to school again; her father's savings were fast dwindling. Supported partly by relatives she went on to study mathematics at college in San Diego, but switched to UC Berkeley, whose mathematics department was then being revamped. After she married Raphael Robinson, she was not able to take up a job as a teacher in the same department, because the university did not allow both husband and wife to work in the same department. This did not bother her much, because the Robinsons were planning to have children and start a family. Unfortunately, Julia lost a baby a couple of months into her pregnancy. When she contracted pneumonia a little later, the doctor who examined her noticed that she had a serious heart problem (probably caused by childhood rheumatic fever), which nobody had noticed earlier. She was told that she could not safely have children any longer; the doctor told her mother that she would not live beyond 40. This disappointed her greatly, and she resumed to work on mathematics to take her mind off her emotional problems. She persevered and worked relentlessly on the Tenth Problem. When she was 41, her heart gave up; she had a successful open heart surgery, and a month later, she bought her first bicycle! A decade later, when she learnt about Matiyasevič's result, the other wish too was fulfilled. Her own contributions to the solution of the Hilbert's Tenth Problem were soon recognized, and she was formally invited to join the faculty of the mathematics department of the UC Berkeley.

After she married Raphael Robinson, she was not able to take up a job as a teacher in the same department, because the university did not allow both husband and wife to work in the same department.

She persevered and worked relentlessly on the Tenth Problem. When she was 41, her heart gave up; she had a successful open heart surgery, and a month later, she bought her first bicycle! A decade later, when she learnt about Matiyasevič's result, the other wish too was fulfilled.

2. Hilbert's Tenth Problem

In his address at the International Congress of Mathematicians in 1900, Hilbert outlined 23 mathematical problems to be studied in the coming century. The Tenth Problem is cited here in full.

> 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*.

What Hilbert refers to as a process according to which an answer is obtained in a finite number of steps is nothing but an *algorithm*, a notion we are all familiar with.

What Hilbert refers to as a process according to which an answer is obtained in a finite number of steps is nothing but an *algorithm*, a notion we are all familiar with. Matiyasevič proved in [2] that the algorithm sought by Hilbert does not exist, thereby providing a negative solution to Hilbert's Tenth Problem. Matiyasevič actually proved that there is no algorithm that, for any given Diophantine equation, determines whether the equation has solutions in the *non-negative integers*. By some simple *reductions*, one can show that this implies the nonexistence of an algorithm to solve Hilbert's original formulation as well. We will only consider non-negative solutions in this article.

2.1 *Diophantine equations, sets, relations, and functions*

A *Diophantine equation* is an equation of the form

$$P(x_1, x_2, \ldots, x_n) = 0,$$

where P is a polynomial with variables from $x_1, \ldots, x_n$ and with integer coefficients. For example,

$$x - (y + 2)(z + 2) = 0 \tag{1}$$

is a Diophantine equation. This equation has many solutions, e.g., including $(x = 16, y = 0, z = 6)$, $(x = 35, y = 3, z = 5)$. The reader will notice that in every solution (x, y, z) of (1), x is a composite number; furthermore, if x is a composite number, then we can find y and z so that (x, y, z) is a solution of (1). In a sense, (1) can be used to *define* the set of composite numbers. More generally, we say that a set $S \subseteq \mathbb{N}$ is a *Diophantine set* if it can be written in the form

$$S = \{x \mid (\exists y_1 \ldots y_n)[P(x, y_1, y_2, \ldots, y_n) = 0]\},$$

where $P(x, y_1, y_2, \ldots, y_n)$ is a polynomial in $n+1$ variables (recall that all variables take values in $\mathbb{N}$). Thus, the following sets are Diophantine (we invite the reader to justify the names of these sets):

$$\begin{aligned} \mathsf{Composites} &= \{x \mid \exists\, y, z\, [x = (y+2)(z+2)]\}; \\ \mathsf{NonPowersOfTwo} &= \{x \mid \exists\, y, z\, [x = y(2z+1)]\}. \end{aligned}$$

(Note that the equations on the right-hand side above have the form $P(x, y, z) = Q(x, y, z)$, which can equivalently be written as $P(x, y, z) - Q(x, y, z) = 0$.) We say that a relation $R \subseteq \mathbb{N}^m$ is a *Diophantine relation* if it can be written in the form

$$R = \{(x_1, \ldots, x_m) \mid (\exists y_1 \ldots y_n)[P(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0]\},$$

where $P(x_1, \ldots, x_m, y_1, \ldots, y_n)$ is a polynomial in $m+n$ variables. Here are some examples of Diophantine relations:

$$\begin{aligned} \mathsf{LessThan} &= \{(x, y) \mid \exists\, z\, [x + z + 1 = y]\}; \\ \mathsf{CongruentModFive} &= \{(x, y) \mid \exists\, z\, [(x - y - 5z)(y - x - 5z) = 0]\}. \end{aligned}$$

We say that a function $f : \mathbb{N}^m \to \mathbb{N}$ is a *Diophantine function* if its graph, namely $G_f = \{(\vec{x}, y) \mid f(\vec{x}) = y\}$, is a Diophantine relation. Consider the Cantor-bijection $\mathsf{cb} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$\mathsf{cb}(x, y) = \frac{(x+y)(x+y+1) + 2y}{2}.$$

This function maps $(0, 0)$ to 0, $(1, 0)$ to 1, $(0, 1)$ to 2, $(2, 0)$ to 3, and so on. The graph of this function is

$$G_{\mathsf{cb}} = \{((x, y), z) \mid 2z = (x+y)(x+y+1) + 2y\},$$

clearly a Diophantine set. The inverse of this function is provided by the following functions left and right, which given a number z, help us to determine the left and right components of the unique pair $(x, y) \in \mathbb{N} \times \mathbb{N}$ such that $\mathsf{cb}(x, y) = z$, that is, for all $z \in \mathbb{N}$, we have $\mathsf{cb}(\mathsf{left}(z), \mathsf{right}(z)) = z$. The graphs of these functions are the Diophantine relations

$$\begin{aligned} G_{\mathsf{left}} &= \{(z, x) \mid \exists y\, [2z = (x+y)(x+y+1) + 2y]\}; \\ G_{\mathsf{right}} &= \{(z, y) \mid \exists x\, [2z = (x+y)(x+y+1) + 2y]\}. \end{aligned}$$

2.2 *Closure properties of Diophantine sets*

In the definition of the relation CongruentModFive, it might have been more natural to ensure that $x = y \pmod{5}$ by checking if at least one of the following two conditions holds: (i) $\exists z\,[5z = x - y]$, (ii) $\exists z[5z = y - x]$; that is, we need a disjunction of two equations. That is, the relation defined CongruentModFive is the union of the relations defined by the individual equations. Such a combination of two equations can be translated to one equation. In general, if P and Q are two polynomials, then $(\exists\vec{y})[P(\vec{x},\vec{y}) = 0]$ *or* $(\exists\vec{y})[Q(\vec{x},\vec{y}) = 0]$ if and only if $(\exists\vec{y})[P(\vec{x},\vec{y}) \cdot Q(\vec{x},\vec{y}) = 0]$. Similarly, $(\exists\vec{y})[P(\vec{x},\vec{y}) = 0]$ *and* $(\exists\vec{y})[Q(\vec{x},\vec{y}) = 0]$ if and only if $(\exists\vec{y})[P(\vec{x},\vec{y})^2 + Q(\vec{x},\vec{y})^2 = 0]$. Thus, Diophantine relations are closed under the operations of union and intersection. They are also closed under projections. Say $S = \{(x, y) \mid \exists\vec{z}\, P(x, y, \vec{z}) = 0\}$ is a Diophantine relation, and $T = \{x \mid \exists y \mid (x, y) \in S\}$. Then, $T = \{x \mid \exists\, y, \vec{z}[P(x, y, \vec{z}) = 0]\}$. We conclude that Diophantine relations are closed under intersection, union, and projection; and if Diophantine relations are combined using an arbitrary sequence of these operations, then the relation that results is also Diophantine. We will see that Diophantine sets are *not* closed under complementation.

2.3 *Recursive functions*

We have seen some examples of Diophantine sets and examined some closure properties that hold for the collection of Diophantine sets. What is the true extent of this collection? The answer is that *a set is Diophantine if and only if it is recursively enumerable!* A set S is *recursively enumerable* (r.e.) if there is a program (written in our favorite programming language) which, when presented with an input $n \in \mathbb{N}$ has two possible behaviors. It performs a finite number of operations and stops with output 1 in case $n \in S$, and it runs forever without stopping if $n \notin S$.

The answer is that *a set is Diophantine if and only if it is recursively enumerable!*

That every Diophantine set is recursively enumerable is not hard to see. For example, consider Diophantine set $S \subseteq \mathbb{N}$ of the form

$\{x \mid \exists y_1, y_2\, P(x, y_1, y_2) = 0\}$. Here is a method that shows that S is r.e.

```
function CHECK(n)                              ▷ Check is n ∈ S
    i ← 0
    while P(n, left(i), right(i)) ≠ 0 do
        i ← i + 1
    end while
    output 1
end function
```

In case $n \in S$, $P(n, y_1, y_2) = 0$ for some choices of values for y_1 and y_2 (say m and p). Then, the loop will terminate when $i = \mathsf{cb}(m, p)$. If $n \notin S$, there are no values of y_1 and y_2 for which the polynomial equation is satisfied, so the loop will run forever and the program will not terminate. If the set was defined using a polynomial of the form $P(x, y_1, y_2, y_3)$, then we would replace the condition in the `while` loop with

$$P(n, \mathsf{left}(\mathsf{left}(i)), \mathsf{right}(\mathsf{left}(i)), \mathsf{right}(i)) \neq 0;$$

the reader can easily imagine what the program would look like if S is defined by a polynomial of the form $P(x, y_1, y_2, \ldots, y_k)$.

It is much harder to show that every r.e. set is Diophantine. We need to start with a rigorous definition of r.e. This could be done in a variety of ways – either by precisely defining idealized computers (*Turing machines*) and how they run programs, or by defining the class of functions computable by those machines (*recursive functions*). Recursive functions are defined inductively by starting with some basic functions (constant functions, successor, the pairing function and its inverses, and some other simple ones), and building new functions from old by means of *function composition*, *iteration*, and *minimization*. Function composition is used to model the execution of statements one after the other in a program (the effects of the individual statements are composed with one another). Iteration, which allows for definitions like $f(n, x) = g^n(x)$, models the execution of a `for` loop, which repeats its body a predetermined number of times. Minimization

Recursive functions are defined inductively by starting with some basic functions (constant functions, successor, the pairing function and its inverses, and some other simple ones), and building new functions from old by means of *function composition*, *iteration*, and *minimization*.

allows for definitions of the following form:

$$f(x) = \text{the smallest } i \text{ such that } g(i, x) = 0.$$

This can be used to compute the number of iterations needed to exit a `while` loop.

One can easily check that the basic functions are all Diophantine, and show that Diophantine functions are closed under composition. Now consider a function f defined by $f(n, x) = g^n(x)$. We can expand this definition as follows:

$$f(n, x) = y \Leftrightarrow \exists y_0 \ldots y_n [y_0 = x \wedge y_n = y \wedge \forall i < n : y_{i+1} = g(y_i)]. \tag{2}$$

The trouble is that the number of quantifiers above is not fixed, so we use a beautiful tool provided by Gödel – *the β-function lemma*. Gödel's β is a Diophantine function of three-variables such that for every n and every sequence of natural numbers $s_0, \ldots, s_n$, there exist two natural numbers a and b such that for all $i \leq n$, $\beta(a, b, i) = s_i$. Using the β-function, we can render (2) as follows.

$$\begin{aligned} f(n, x) = y \Leftrightarrow \exists a, b\, [\beta(a, b, 0) = x \wedge \beta(a, b, n) = y \\ \wedge\, \forall i < n : \beta(a, b, i + 1) = g(\beta(a, b, i))]. \end{aligned}$$

When we consider a function f defined by minimization from g, we see that $f(x) = i$ if and only if $g(i, x) = 0$ and $\forall j < i$: $\exists y\, [g(j, x) = y + 1]$. We already know that we can translate disjunction, conjunction, and existential quantification over Diophantine equations into another Diophantine equation. If we can somehow also show closure of Diophantine equations under *bounded universal quantification* (i.e., if the set $S \subseteq \mathbb{N}^2$ is Diophantine, then so is $T = \{(x, n) \mid \forall i < n : (x, i) \in S\}$), then we can conclude that Diophantine sets are closed under iteration and minimization, and that all recursive functions are Diophantine. It will follow that all r.e. sets are Diophantine.

3. Exponential Diophantine Equations and Unsolvability

From the discussion so far, we see that the major challenge that remains is to show closure of Diophantine sets under bounded universal quantification. Several partial results were obtained by Martin Davis and Hilary Putnam, and independently by Julia Robinson, which culminated in their joint paper [3]. In this, they showed that *if* we assume that the exponential function is Diophantine, then Diophantine sets are closed under bounded universal quantification.[1] The proof is not simple by any means, and involves providing Diophantine equations for a dizzying array of functions like the $n!$, $\binom{n}{k}$ and $\prod_{k=0}^{n}(a + bk)$, and finally, bounded universal quantification.

We thus arrive at the conclusion that a set is r.e. iff it is Diophantine. We have reached the endgame now. It is well-known (an elementary result in computability theory, see [4]) that there is an r.e. set H whose complement $\overline{H} = \mathbb{N} \setminus H$ is not r.e. This, incidentally, shows that the class of Diophantine sets is not closed under complementation. Since H is r.e., it is Diophantine, say it is described by a polynomial P_H:

$$H = \{n \mid \exists\vec{y}\,[P_H(n, \vec{y}) = 0]\}.$$

Now, suppose there were a program to solve Hilbert's Tenth Problem. Then, there would be an algorithm A that when presented with a polynomial equation, would after a finite number of steps, halt and produce a result of 1 or 0: 1 if the polynomial has a solution and 0 otherwise. In particular, A can answer correctly for the polynomials in the list

$$P_H(0, \vec{y}), P_H(1, \vec{y}), P_H(3, \vec{y}), \ldots, P_H(n, \vec{y}), \ldots.$$

Now, using A, build a program B that works as follows. On input n, B calls A with input $P_H(n, \vec{y})$, and if A returns 1, B would enter an endless loop, while if A returns 0, B returns 1. But this would mean that $\overline{H}$ is r.e. – a contradiction. This proves that program A with the stated behavior cannot exist, and hence Hilbert's Tenth Problem is unsolvable!

[1]Sets that are defined by Diophantine equations which involve the exponential function are called *exponential Diophantine*.

4. Defining the Exponential – Julia Robinson and Matiyasevič

The above results were obtained assuming that the exponential function is Diophantine. In fact, Julia Robinson gave another assumption which would imply that the exponential is Diophantine.[2] She showed that if one assumes the existence of a Diophantine set $D \subseteq \mathbb{N}$ with the following properties, then the exponentiation function is Diophantine:

1. $\mathsf{cb}(u, v) \in D \Rightarrow v \leq u^u$.
2. $\forall k \exists u, v\,[\mathsf{cb}(u, v) \in D \wedge v > u^k]$.

Matiyasevič showed that the Fibonacci numbers satisfy very similar growth properties to the D above, using which he constructed a Diophantine representation for the exponentiation function. Subsequently, it was shown (with contributions from Julia herself) that the set of solutions of the so-called *Brahmagupta equation* satisfies the properties of D listed above, thus providing a solution to Hilbert's Tenth Problem following Julia Robinson's template almost entirely.

Subsequently, it was shown (with contributions from Julia herself) that the set of solutions of the so-called *Brahmagupta equation* satisfies the properties of *D* listed above, thus providing a solution to Hilbert's Tenth Problem following Julia Robinson's template almost entirely.

To learn more about Hilbert's Tenth Problem and its unsolvability, one can consult the excellent article by Martin Davis [5] or the delightful book by Ram Murthy and Fodden [6], which is a thorough and self-contained account of the problem and the solution.

Suggested Reading

[1] Constance Reid, The autobiography of Julia Robinson, *College Math. J.*, Vol.17, No.1, pp.3–21, 1986. DOI: 10.1080/07468342.1986.11972925

[2] Yuri Matiyasevič, Enumerable sets are Diophantine, *Doklady Akad. Nauk SSSR*, Vol.191, pp.279–282, 1970. Improved English translation: *Soviet Math. Doklady*, Vol.11, pp.354–357, 1970.

[3] Martin Davis, Hilary Putnam and Julia Robinson, The decision problem for exponential Diophantine equations, *Ann. Math.*, Vol.74, pp.425–436, 1961.

[2]This is the Robinson Hypothesis mentioned in Section 1.

[4] A Shen and N K Vereshchagin, Computable Functions, AMS Student Mathematical Library, American Mathematical Society, Providence, RI 02904-2213, USA, Vol.19, 166 pages, 2003.

[5] Martin Davis, Hilbert's tenth problem is unsolvable, *Am. Math. Mon.*, Vol.80, No.3, pp.233–269, 1973.

[6] M Ram Murthy and Brandon Fodden, Hilbert's Tenth Problem: An Introduction to Logic, Number Theory, and Computability, American Mathematical Society, Providence, RI 02904-2213, USA, 239 pages, 2019.

Address for Correspondence
Jaikumar Radhakrishnan
International Centre for Theoretical Sciences (ICTS),
Shivakote, Hesaraghatta Hobli,
Bengaluru 560 089, India
Email:
jaikumar.radhakrishnan@icts.res.in

S P Suresh
Chennai Mathematical Institute,
H1, SIPCOT IT Park, Siruseri,
Kelambakkam 603 103, India
Email: spsuresh@cmi.ac.in