Hilbert's tenth problem

Ananya Sriram and Jisha Rajala

December 2022

1 Introduction

In 1900, David Hilbert published a list of perceived unsolvable questions in mathematics, the tenth of which was Hilbert's tenth problem, stating the following (6):

> "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 in a finite number of operations whether the equation is solvable in rational integers."

In other words, Hilbert looked for a solution, such that if given a Diophantine equation with any number of unknown quantities with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers (1).

Hilbert's problem is more concerned with deciding whether one or more solutions exist to a certain set of Diophantine equations. Mathematician The Yuri Matiyasevich derived that the solution to the problem is negative in 1970, meaning that there is no algorithm that can be devised to answer the question (1).

The following paper will explore the definition of Diophantine sets and equations, along with Matiyasevich's proof, and overall applications of the problem.

2 Computability theory

In order to make sense of the negative result of Hilbert's Tenth Problem, we need to develop a precise notion of algorithms. In the 1930s, the Church-Turing thesis proved that every purely mechanical procedure could be carried out by a Turing Machine, a model of computation.

Definition 1.1: A Turing Machine is an abstract computing machine used to determine the limitations of what can and cannot be computed.

Hilbert's Tenth Problem can be rephrased to ask whether there exists a Turing machine that can solve the decision problem of whether one or more solutions exist for an input set of polynomial equations.

Definition 1.2: A subset S of N is called recursive if there exists a Turing Machine accepting a natural number n and is guaranteed to terminate after running for a finite amount of time, after which it correctly outputs the truth value(Yes or No) according to whether n S.

Definition 1.3: A subset S of N is called listable or recursively enumerable if there exists a Turing Machine accepting a natural number n and, if n S, the algorithm need not be guaranteed to terminate for inputs n S, but must not give any incorrect answers.

It is clear that recursively enumerable sets are not required to terminate if the input is not in the solution set S, unlike recursive sets, which always terminate on any input. However, it is not immediately clear that the set of recursively enumerable sets that are not also recursive is nonempty. This property is justified by the following theorem:

Theorem 1.1: A simple set is a set that is both co-infinite and recursively enumerable but any infinite subset of its complement is not recursively enumerable. Simple sets are not recursive.

Proof : Suppose that S is a simple set, implying that it is both co-infinite and recursively enumerable.

Now, suppose that S is recursive. Then, there exists an algorithm, a, that can determine, for any given integer x, whether x is in S or not. Using this information, the following algorithm can be used to enumerate the elements of *S'*:

1. Initialize an empty list L.
2. For each x in the domain of the algorithm, a, if a decides that x is not in S, append x to L.
3. Output L

Since *S'* is infinite, this algorithm will never terminate. However, S is recursively enumerable, meaning that there exists an algorithm that can enumerate all of the elements in S in a systematic way, suggesting that this algorithm has to output L, which poses a contradiction. Therefore, S cannot be recursive.

3 The Halting Problem

The Halting Problem asks if there exists a Turing Machine such that it accepts a computer program p and integer x and output *YES* or *NO* based on whether the program eventually halts when run on the integer, x.

Theorem 2.1: The Halting Problem is undecidable (cannot be solved by any Turing machine)

$Proof$: Suppose there exists a Turing machine M that can solve the Halting Problem. Then, M can be used to construct a new Turing machine H that takes a description of a Turing machine M and an integer w as inputs and halts only if *M'* halts when run on w.

Consider the following program P:

1. Input a description of a Turing machine *M'* and an input w.
2. Run H on *M'* and w.
3. If H halts, halt. Otherwise, loop forever.

If P halts when run on itself, then it must halt when run on H. However, if P halts when run on H, then H must halt when run on P. This can be summarized as *P(p)* will halt if and only if the program *P(p)* will run forever, which is a contradictory statement, resulting in the conclusion that The Halting Problem is undecidable.

Corollary 2.1 Listable sets are not always recursive(i.e. there exists a listable set that is not recursive

$Proof$: Consider the set L of all descriptions of Turing machines M such that M does not halt when run on itself

It is possible to enumerate all of the elements in the set L using the following algorithm:

1. Initialize an empty list *L'*.
2. If M does not halt when run on itself, append M to *L'*.
3. Output *L'*.

This algorithm will enumerate all of the elements in the set *L'* in a systematic way, so L is a listable set. However, L is not recursive because the definition of L depends on the behavior of Turing machines, which is not something that can be determined algorithmically.

4 An Introduction to Diophantines

The first step to approaching Hilbert's Tenth Problem is getting a grasp for the concept of Diophantine equations. In basic terms, a Linear Diophantine equation (LDE) is an equation with atleast 2 unknowns, such that each unknown represents an integer value and are each to at most degree of 1.

We can proceed to define Diophantine sets and equations as follows:

Definition 4.1: A set S of ordered n-tuples of positive integers is called a Diophantine set if there is a polynomial $P(x_l, ..., x_n, y_1, ..Y_m)$, where $m \geq 0$, with integer coefficients such that a given *n-tuple $< x_1, ..., x_n >$ belongs to S if and only if there exist positive integers $Y_1, ..., y_m$ such that $P(x_1, ..., x_n, y_1, ..Y_m) = 0$.

So, $S = \{< x_1, ..., x_n > |\exists(y_1, ..., Y_m)[P(x_1, ..., x_n, y_1, ..Y_m) = 0\}$

What are some examples of Diophantine sets that satisfy this definition?

The composite numbers, for one, which can be defined as

$$S = \{x = (y + 1)(z + 1)\}$$

for $x \in S$ and $y, z \in \mathbb{Z}$

Diophantine equations and closely related to Diophantine sets.

Definition 4.2: Let $P(x_1, ..., x_m)$ be the polynomial from **definition 1.1** with only integer unknown values of $x_1, ...x_m$ and integer coefficients. If an equation satisfies this, $P(x_1, ..., x_m) = 0$ it is a Diophantine equation. Similarly, if there is a Diophantine set S as defined in **definition 1.1**, then set S has a dimension of m and the polynomial P is the Diophantine representation of the set S.

And while this defines the Diophantine sets and equations, they have more properties and operations that can contribute to proving Hilbert's tenth problem as negative.

Theorem 4.1 The union of two Diophantine sets of the same dimension is Diophantine.

Proof : Say there exist Diophantine sets S_a and S_b such that the two sets have representations of P_a and P_b. The union of the two Diophantine sets is a new polynomial $P_a \cdot P_b$, as $P_a \cdot P_b = 0$ if and only if $P_a = 0$ and $P_b = 0$. Based on our definition of Diophantine sets, we now know that this is Diophantine.

Theorem 4.2 The intersection of two Diophantine sets is Diophantine.

Proof : Say there exist Diophantine sets S_a and S_b such that the two sets have representations of P_a and P_b. The intersection of the two Diophantine sets is a new polynomial $(P_a)^2 + (P_b)^2$, as $(P_a)^2 + (P_b)^2$ if and only if $P_a = 0$ and $P_b = 0$. Based on our definition of Diophantine sets, we now know that this is Diophantine.

Theorem 4.3 All recursively enumerable set in the natural numbers are Diophantine, and therefore the converse: a subset in the natural numbers is Diophantine if and only if it is recursively enumerable.

Proof : This theorem is known as the DPRM theorem, named after Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matiyasevich's work on Hilbert's Tenth Problem. The proof for the theorem itself is very technical, however we will delve into the basics of it in section 5.

Lemma 4.1 Hilbert's Tenth problem has a negative answer.

Proof : For the sake of contradiction, let us say that there exists a subset S of the set integers $\mathbb{Z}$ such that S is non-recursive but listable (Corollary 2.1). By the DPRM theorem, we know that this same subset S is Diophantine as well.

Therefore, we know that there must exist a polynomial $P(x_1, ..., x_n, y_1, ..Y_m)$ such that

$$S = \{< x_1, ..., x_n > | \exists (y_1, ..., Y_m)[P(x_1, ..., x_n, y_1, ..Y_m) = 0\}$$

and $P(x_1, ..., x_n, y_1, ..Y_m) = 0$.

For the sake of contradiction, let's say that Hilbert's Tenth Problem actually has a negative answer. Then, there should be an algorithm that can decide whether there exists a solution $(y_1, ..., Y_m)$ in the natural numbers.

Based on this, we would be able to decide if $< x_1, ..., x_n > \in S$, meaning that S is recursive. Therefore, based on this contradiction, we know that Hilbert's tenth problem must have a negative solution, meaning that there is no deciding algorithm.

5 DRMP theorem

The following section will work to establish a basic proof and outline of the DRMP theorem utilized to show that Hilbert's Tenth Problem is unsolvable. The DRMP theorem is the most crucial part to the problem besides a basic definition of Diophantines.

The proof below will include the basics of the proof, not delving too much into the further complexities of the theorem.

Basic Outline

The proof of the theorem consists of the following:

- Show every listable set is exponential Diophantine
- Show exponentiation is Diophantine
- Show different relations that are Diophantine

6 All listable sets are exponential Diophantine

An exponential Diophantine is a Diophantine set or equation in which the unknown solutions may also appear in the exponents of the polynomial.

The proof itself is extremely complex, and was proven by Davis, Putnam, and Robinson in 1960 (2). While the proof will not be shown in this paper, Davis, Putnam, and Robinson utilized the idea that the listable set S can be expressed as the linear combination of the products of terms in the form of α^{β}. As there are nonrecursive and listable sets, the new listable set can expressed in terms of a exponential Diophantine equation.

However, their proof brings up other new corollaries relevant to Hilbert's Tenth Problem.

Corollary 1 There exists no algorithm that determines whether an exponential Diophantine is unsolvable.

Their proof for the following corollary is similar to Theorem 4.3 which shows that the solution to Hilbert's tenth problem is negative.

Research shows that while many exponential Diophantines can be solved using Størmer's theorem or trial and error, no specific pattern or algorithm has been devised to determine whether there exist solutions to an exponential Diophantine.

Some examples of interesting exponential Diophantines are the Fermat-Catalan conjecture (4):

$a^m + b^n = c^k$ has only finitely many solutions such that a,b,c are coprime and

$$\frac{1}{m} + \frac{1}{n} + \frac{1}{k} < 1.$$

and the Ramanujan-Nagell equation (7):

$$2^n - 7 = x^2.$$

7 Exponentiation is Diophantine

To show that exponentiation is Diophantine, we must show that the ordered set of triples, $a, b, c | a = b^c$ is a Diophantine set.

Interestingly, a clever solution to this is to use Pell's equation of $x^2 - dy^2 = 1$ for a non-square d in the natural numbers. Robinson's work on proving that exponentiation is Diophantine involved Pell's equation to prove that

> "There is a Diophantine set D of pairs (a,b) such that $(a, b) \in D \Rightarrow b < a^a$ and for every positive k, there exists $(a, b) \in D$ such that $b > a^k$. (1)"

In this proof, Robinson also implies that not only is exponentiation Diophantine, so are the binomial coefficients, factorials, and primes (2).

Exponential growth as a Diophantine relation is key to the unsolvability of Hilbert's Tenth Problem. Constructing a Diophantine such that the solutions showcase exponential growth would make the problem undecidable by an algorithm. The discovery of this equation allows any exponential Diophantine to become a linear Diophantine equation, therefore making Hilbert's Tenth Problem negative.

8 Hilbert's Tenth Problem in other rings

While Hilbert's Tenth Problem originally deals with only integers, the problem can be extended to a variety of other mathematical rings, each with their own solutions to the problem. While the problem is undecided in the rational numbers, it has been solved in other rings.

The table below showcases the solutions to the problem in different rings of interest.

HB10 in other rings	
Ring	Is there a solution to HB10?
$Q(\sqrt{d})$ (3)	yes; negative
Q	not known
p-adic (8)	yes; positive
$\mathbb{Z}$	yes; negative
$\mathbb{O}_K$ (10)	not known
$\mathbb{C}$	yes; positive
$\mathbb{Z}[i]$	yes; negative

As a generalization for different rings, Harold N. Shapiro and Alexandra Shlapentokh proved in 1989 that the problem has a negative solution for integer rings of any algebraic number field such that the Galois group over the rationals is abelian (11).

The study of Hilbert's Tenth Problem in different rings extends it to the work in areas of interest of various number theorists and algebraists, also extending the applications of the problem itself to different fields of mathematics.

9 Applications

One application of Hilbert's 10th Problem is in the field of algebraic geometry, where it can be used to prove the existence of certain types of algebraic varieties that cannot be described by polynomial equations. Specifically, the proof that there does not exist an algorithm that can solve Hilbert's 10th Problem for all polynomial equations has been used to show that there exist algebraic varieties that cannot be defined by polynomial equations with integer coefficients (9).

Another application of Hilbert's 10th Problem is in the field of computational complexity theory, where it has been used to establish the existence of certain types of computational problems that are computationally intractable, meaning it requires a very large amount of computational resources to solve. Specifically, the proof that there does not exist an algorithm that can solve Hilbert's 10th Problem has been used to show that there exist computational problems that are hard to solve, in the sense that they require a lot of computational resources to solve, even with the most powerful computational resources.

10 Acknowledgements

We would like to thank Simon Rubinstein-Salzedo, Aditi Taliti, Aaron Lin, and Euler Circle for providing us with the opportunity to write this paper, research Theory of Computation, and endless guidance in the process of learning about the field.

11 references

1. Davis, M. (1973). Hilbert's Tenth Problem is Unsolvable. The American Mathematical Monthly, 80(3), 233–269. https://doi.org/10.2307/2318447

2. Davis, M., Putnam, H., Robinson, J. (1961). *The Decision Problem for Exponential Diophantine Equations.* Annals of Mathematics, 74(3), 425–436. https://doi.org/10.2307/1970289

3. Denef, J. (1975). *Hilbert's Tenth Problem for Quadratic Rings.* Proceedings of the American Mathematical Society, 48(1), 214–220. https://doi.org/10.2307/2040720

4. Ghannouchi, J. (2014). *An elementary proof of Fermat-Catalan conjecture.* https://hal.archives-ouvertes.fr/hal-00966840v4

5. Ho, A. J. (2015). *Hilbert's tenth problem.* https://sites.math.washington.edu/ morrow/336_15/papers/andrew.pdf

6. Matiyasevich, Y.V. (1933). *Hilbert's Tenth Problem.* Cambridge: MIT Press.

7. Mead, D. G. (1973). *The Equation of Ramanujan-Nagell and [y2]. Proceedings of the American Mathematical Society*, 41(2), 333–341. https://doi.org/10.2307/2039090

8. Nerode, A. (1963) *A decision method for p-adic integral zeros of diophantine equations.* Bull. Amer. Math. Soc, 69, 513–517.

9. Pheidas, T. (1994). *Extensions of Hilbert's Tenth Problem.* The Journal of Symbolic Logic, 59(2), 372–397. https://doi.org/10.2307/2275396

10. Poonen, B. (2003). *Hilbert's Tenth Problem over Rings of Number-Theoretic Interest.* http://www-math.mit.edu/ poonen/papers/aws2003.pdf

11. Shapiro, H.N., Shlapentokh, A. (1989). *Diophantine Relationships Between Algebraic Number Fields.* 42(8), 1113-1122. https://doi.org/10.1002/cpa.3160420805