

# Hilbert's Tenth Problem

Frank Patane

Foundations of Mathematics  
[www.math.ufl.edu/~frankpatane](http://www.math.ufl.edu/~frankpatane)

April 11, 2011

Outline

A Brief  
History

Basic  
Concepts

H10  
Generalized

References

① A Brief History

② Basic Concepts

③ H10 Generalized

④ References

## A Brief History

In 1900, at the International Congress of mathematicians, David Hilbert presented a list of problems that was to guide the mathematics community for the coming century.

## A Brief History

In 1900, at the International Congress of mathematicians, David Hilbert presented a list of problems that was to guide the mathematics community for the coming century.



# A Brief History

The tenth problem on Hilbert's list of 23 problems states:

## A Brief History

The tenth problem on Hilbert's list of 23 problems states:

"Find an algorithm to determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution."

# A Brief History

The tenth problem on Hilbert's list of 23 problems states:

"Find an algorithm to determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution."

In 1970 Matijasevic proves that no such algorithm can exist using the work of Davis-Putnam-Robinson.

# Basic Concepts

More generally one could ask for an algorithm for solving a system of diophantine equations.

# Basic Concepts

More generally one could ask for an algorithm for solving a system of diophantine equations.

Noting that  $f_1 = f_2 = \dots = f_n = 0$  iff  $f_1^2 + f_2^2 + \dots + f_n^2 = 0$  we see that finding an algorithm for solving a system of diophantine equations is equivalent to Hilbert's tenth problem.

## Basic Concepts

More generally one could ask for an algorithm for solving a system of diophantine equations.

Noting that  $f_1 = f_2 = \dots = f_n = 0$  iff  $f_1^2 + f_2^2 + \dots + f_n^2 = 0$  we see that finding an algorithm for solving a system of diophantine equations is equivalent to Hilbert's tenth problem.

As an exercise, show that if there is no algorithm for finding whether a diophantine equation has positive solutions, then Hilbert's tenth problem is proved in the negative. As a hint, think of Lagrange four squares theorem.

**Definition:**  $A \subset \mathbb{N}^k$  is called a **Diophantine set** if there exists a polynomial  $p \in \mathbb{Z}[y_1, \dots, y_k, x_1, \dots, x_m]$  such that  $(a_1, \dots, a_k) \in A$  iff there exists  $x_1, \dots, x_m \in \mathbb{N}$  such that  $p(a_1, \dots, a_k, x_1, \dots, x_m) = 0$ .

## Basic Definitions

**Definition:**  $A \subset \mathbb{N}^k$  is called a **Diophantine set** if there exists a polynomial  $p \in \mathbb{Z}[y_1, \dots, y_k, x_1, \dots, x_m]$  such that  $(a_1, \dots, a_k) \in A$  iff there exists  $x_1, \dots, x_m \in \mathbb{N}$  such that  $p(a_1, \dots, a_k, x_1, \dots, x_m) = 0$ .

We will call the elements of a diophantine set the **parameters** of the polynomial.

## Basic Definitions

**Definition:**  $A \subset \mathbb{N}^k$  is called a **Diophantine set** if there exists a polynomial  $p \in \mathbb{Z}[y_1, \dots, y_k, x_1, \dots, x_m]$  such that  $(a_1, \dots, a_k) \in A$  iff there exists  $x_1, \dots, x_m \in \mathbb{N}$  such that  $p(a_1, \dots, a_k, x_1, \dots, x_m) = 0$ .

We will call the elements of a diophantine set the **parameters** of the polynomial.

So considering the Pellian equation  $x^2 - d(y + 1)^2 = 1$  over  $\mathbb{N}$  we know that this equation will be solvable exactly when  $d$  is 0 or not a perfect square.

## Basic Definitions

**Definition:**  $A \subset \mathbb{N}^k$  is called a **Diophantine set** if there exists a polynomial  $p \in \mathbb{Z}[y_1, \dots, y_k, x_1, \dots, x_m]$  such that  $(a_1, \dots, a_k) \in A$  iff there exists  $x_1, \dots, x_m \in \mathbb{N}$  such that  $p(a_1, \dots, a_k, x_1, \dots, x_m) = 0$ .

We will call the elements of a diophantine set the **parameters** of the polynomial.

So considering the Pellian equation  $x^2 - d(y + 1)^2 = 1$  over  $\mathbb{N}$  we know that this equation will be solvable exactly when  $d$  is 0 or not a perfect square.

Thus the set of natural numbers that include 0 and all non-square integers is a Diophantine set.

## Basic Definitions

**Definition:**  $A \subset \mathbb{N}^k$  is called a **Diophantine set** if there exists a polynomial  $p \in \mathbb{Z}[y_1, \dots, y_k, x_1, \dots, x_m]$  such that  $(a_1, \dots, a_k) \in A$  iff there exists  $x_1, \dots, x_m \in \mathbb{N}$  such that  $p(a_1, \dots, a_k, x_1, \dots, x_m) = 0$ .

We will call the elements of a diophantine set the **parameters** of the polynomial.

So considering the Pellian equation  $x^2 - d(y + 1)^2 = 1$  over  $\mathbb{N}$  we know that this equation will be solvable exactly when  $d$  is 0 or not a perfect square.

Thus the set of natural numbers that include 0 and all non-square integers is a Diophantine set.

Can anyone think of another Diophantine set?

## Basic Definitions

**Definition:**  $A \subset \mathbb{N}$  is **recursively enumerable** if there is a Turing machine such that  $A$  is the set that it prints out if left running forever. (This is from Definition 5.21 in the class notes.)

## Basic Definitions

**Definition:**  $A \subset \mathbb{N}$  is **recursively enumerable** if there is a Turing machine such that  $A$  is the set that it prints out if left running forever. (This is from Definition 5.21 in the class notes.)

**Definition:**  $A \subset \mathbb{N}$  is recursive if there is an algorithm which terminates after a finite amount of time and correctly determines whether or not a given integer is in  $A$  or not. (Again Definition 5.21)

## Basic Definitions

**Definition:**  $A \subset \mathbb{N}$  is **recursively enumerable** if there is a Turing machine such that  $A$  is the set that it prints out if left running forever. (This is from Definition 5.21 in the class notes.)

**Definition:**  $A \subset \mathbb{N}$  is recursive if there is an algorithm which terminates after a finite amount of time and correctly determines whether or not a given integer is in  $A$  or not. (Again Definition 5.21)

Is a Diophantine set necessarily recursively enumerable?

**Definition:**  $A \subset \mathbb{N}$  is **recursively enumerable** if there is a Turing machine such that  $A$  is the set that it prints out if left running forever. (This is from Definition 5.21 in the class notes.)

**Definition:**  $A \subset \mathbb{N}$  is recursive if there is an algorithm which terminates after a finite amount of time and correctly determines whether or not a given integer is in  $A$  or not. (Again Definition 5.21)

Is a Diophantine set necessarily recursively enumerable?

Yes! Take a Diophantine equation  $f(a, x_1, \dots, x_k) = 0$ , and make an algorithm that tries all possible values of  $a, x_1, \dots, x_k$  and prints  $a$  whenever  $f(a, x_1, \dots, x_k) = 0$ .

# Observations

Any recursive set is recursively enumerable.

# Observations

Any recursive set is recursively enumerable.

However there exists recursively enumerable sets that are not recursive.

# Observations

Any recursive set is recursively enumerable.

However there exists recursively enumerable sets that are not recursive.

Yet is it true that any recursively enumerable set is Diophantine?

## Observations

Any recursive set is recursively enumerable.

However there exists recursively enumerable sets that are not recursive.

Yet is it true that any recursively enumerable set is Diophantine?

Yes! Matiyasevich's Theorem is that a set of integers is Diophantine if and only if it is recursively enumerable.

## Observations

Any recursive set is recursively enumerable.

However there exists recursively enumerable sets that are not recursive.

Yet is it true that any recursively enumerable set is Diophantine?

Yes! Matiyasevich's Theorem is that a set of integers is Diophantine if and only if it is recursively enumerable.

But how exactly does this prove Hilbert's tenth problem?

# H10 as a Corollary

Fact 1: Some recursively enumerable sets are not recursive.(1930s)

## H10 as a Corollary

Fact 1: Some recursively enumerable sets are not recursive.(1930s)

Fact 2: Matiyasevich's Theorem states that all recursively enumerable sets are Diophantine sets.(1970)

## H10 as a Corollary

Fact 1: Some recursively enumerable sets are not recursive.(1930s)

Fact 2: Matiyasevich's Theorem states that all recursively enumerable sets are Diophantine sets.(1970)

Conclusion: There exist some Diophantine sets that are not recursive.

## H10 as a Corollary

Fact 1: Some recursively enumerable sets are not recursive.(1930s)

Fact 2: Matiyasevich's Theorem states that all recursively enumerable sets are Diophantine sets.(1970)

Conclusion: There exist some Diophantine sets that are not recursive.

In other words, there is a Diophantine equation depending on a parameter for which no algorithm can decide for which values of the parameter the equation has a solution.

# H10 Generalized

We can generalize H10 to other integral domains.

# H10 Generalized

We can generalize H10 to other integral domains.

Let  $R$  be an integral domain. Then H10 over  $R$  is the question,

## H10 Generalized

Outline

A Brief  
HistoryBasic  
ConceptsH10  
Generalized

References

We can generalize H10 to other integral domains.

Let  $R$  be an integral domain. Then H10 over  $R$  is the question,

Is there an algorithm with

input:  $f(x_1, x_2, \dots, x_n) \in R[x_1, \dots, x_n]$

output: Yes or no, according to whether there exists  
 $a_1, \dots, a_n \in R$  such that  $f(a_1, a_2, \dots, a_n) = 0$ .

# H10 Generalized

Doing a bit of research we find that H10 over  $R = \mathbb{C}, \mathbb{R}, \mathbb{Q}_p$  has been solved in the positive by using "elimination theory." [5]

Outline

A Brief  
History

Basic  
Concepts

H10  
Generalized

References

## H10 Generalized

Doing a bit of research we find that H10 over  $R = \mathbb{C}, \mathbb{R}, \mathbb{Q}_p$  has been solved in the positive by using "elimination theory." [5]

However the above mentioned  $R$  are all fields. A closer situation of H10 as originally stated might take  $R$  to be just a unique factorization domain or maybe even a Dedekind domain.

## H10 Generalized

Doing a bit of research we find that H10 over  $R = \mathbb{C}, \mathbb{R}, \mathbb{Q}_p$  has been solved in the positive by using "elimination theory." [5]

However the above mentioned  $R$  are all fields. A closer situation of H10 as originally stated might take  $R$  to be just a unique factorization domain or maybe even a Dedekind domain.

The obvious generalization is to take a number field  $K$  and set  $R$  equal to the ring of integers of  $K$ .

## H10 Generalized

Doing a bit of research we find that H10 over  $R = \mathbb{C}, \mathbb{R}, \mathbb{Q}_p$  has been solved in the positive by using "elimination theory." [5]

However the above mentioned  $R$  are all fields. A closer situation of H10 as originally stated might take  $R$  to be just a unique factorization domain or maybe even a Dedekind domain.

The obvious generalization is to take a number field  $K$  and set  $R$  equal to the ring of integers of  $K$ .

So we could have  $R$  being the Gaussian integers or Eisenstein integers, for instance.

## H10 Generalized

Doing a bit of research we find that H10 over  $R = \mathbb{C}, \mathbb{R}, \mathbb{Q}_p$  has been solved in the positive by using "elimination theory." [5]

However the above mentioned  $R$  are all fields. A closer situation of H10 as originally stated might take  $R$  to be just a unique factorization domain or maybe even a Dedekind domain.

The obvious generalization is to take a number field  $K$  and set  $R$  equal to the ring of integers of  $K$ .

So we could have  $R$  being the Gaussian integers or Eisenstein integers, for instance.

**Conjecture:** H10 has a negative answer for the ring of integers for any number field.

# You've Got Problems!

Outline

A Brief  
History

Basic  
Concepts

H10  
Generalized

References

1.) Let  $A, B$  be Diophantine sets. Show that  $A \cup B$  and  $A \cap B$  are Diophantine sets. Is the complement of  $A$  necessarily Diophantine?

# You've Got Problems!

Outline

A Brief  
History

Basic  
Concepts

H10  
Generalized

References

- 1.) Let  $A, B$  be Diophantine sets. Show that  $A \cup B$  and  $A \cap B$  are Diophantine sets. Is the complement of  $A$  necessarily Diophantine?
- 2.) Find a Diophantine equation that has no non-negative integer solutions, yet has infinitely many integer solution. Why does this not contradict the "exercise" mentioned on slide 5?

# You've Got Problems!

Outline

A Brief  
History

Basic  
Concepts

H10  
Generalized

References

- 1.) Let  $A, B$  be Diophantine sets. Show that  $A \cup B$  and  $A \cap B$  are Diophantine sets. Is the complement of  $A$  necessarily Diophantine?
- 2.) Find a Diophantine equation that has no non-negative integer solutions, yet has infinitely many integer solution. Why does this not contradict the "exercise" mentioned on slide 5?
- 3.) Complete the claim that  $x^2 - d(y + 1)^2 = 1$  is solvable in  $\mathbb{N}$  iff  $d = 0$  or  $d$  is not a perfect square.

## References

Thank you, and I hope you are inspired to look into H10!

Outline

A Brief  
History

Basic  
Concepts

H10  
Generalized

References

## References

Thank you, and I hope you are inspired to look into H10!

### References:

- [1.] Shlapentokh, A. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press, 2007.
- [2.] Matijasevich, U. *Hilbert's Tenth Problem*. MIT Press, 1993.
- [3.] Sussmann, H J. *Hilbert's Tenth Problem*. 1971
- [4.] Rogers, H. *Theory of Recursive Functions and Effective Computability*. MIT Press, 1987.
- [5.] Poonen, Bjorn. *Hilbert's Tenth Problem*. MSRI Introductory Workshop on Rational and Integral Points on Higher-dimensional Varieties 2006