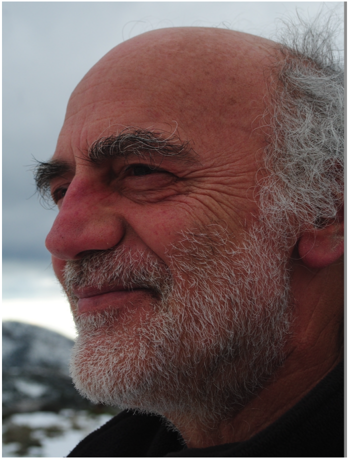
# The Mathematics of Thanasis Pheidas



Presented for an audience that includes non-mathematicians

by Lefteris Kirousis
of the National and Kapodistrian University of Athens

# Infinity

## Question

How can we determine that two sets have an equal number of elements, *without counting them?*

## Answer

Like kindergarden children do: by juxtaposing their elements without leaving out any elements from any of the sets. Technical terminology: by defining between the sets a one-to-one correspondence.

## Question

What is an infinite set?

## Answer

One that has an equal number of elements with a strict (proper) subset of it.

# More about infinite sets

- An example of an infinite set known to everybody: the set of nonnegative whole numbers (natural numbers) $\mathbb{N} = \{0, 1, 2, \ldots\}$

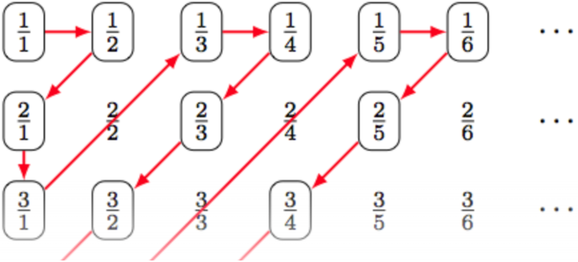
$$
\begin{gathered}
0 \leftrightarrow 0 \\
1 \leftrightarrow 2 \\
2 \leftrightarrow 4 \\
\vdots \\
n \leftrightarrow 2n \\
\vdots
\end{gathered}
$$

# Countable sets

**Definition**

Countable sets are the ones whose elements can be listed one after the other (not necessarily in order of their size). In other words are either finite or have the same number of elements as the natural numbers

- An example: the set of fractions of positive natural numbers ($Q$: positive rational numbers):



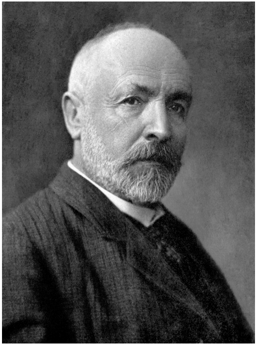
# Do uncountable sets exist?

- YES!

The set of real numbers $\mathbb{R}$, which is comprised of:

- the rational numbers, plus
- the algebraic numbers (solutions of equations with integer coefficients) like $\sqrt{2}$ (all these are countable), plus
- the non-algebraic numbers like $\pi$, the quotient of the perimeter of any circle over its diameter. The latter are the vast majority.

# How do we know that the set of real numbers is uncountable?



Georg Cantor 1845–1918

The diagonal method: Suppose that you could juxtapose with the whole positive numbers the set of all positive real numbers less than 1.

$$1 \leftrightarrow 0.148587\cdots$$
$$2 \leftrightarrow 0.932176\cdots$$
$$3 \leftrightarrow 0.811234\cdots$$
$$\vdots$$

Construct a new real number $\mathrm{diag} = 0.212\cdots$ different from all numbers in the list moving along the diagonal and changing the $n$-th decimal digit of the $n$-number in the list.

# Self-referential statements

- At the previous argument in order to construct the number $\mathrm{diag}$ we "belied" the $n$-th decimal digit of the $n$-th number in the list.

- This is, in some sense, a formal way of putting the liar paradox, a self-referential statement:


Epimenides 7th – 6th century BCE

Epimenides, the Cretan , says, "Cretans are liars", which leads to a vicious circle of contradictions (under the assumption that all Cretans are always truthful or all Cretans are always liars).

# The power of natural numbers

L. Kronecker: God created the natural numbers; all the rest is the work of man.

### Important fact

All finite mathematical objects like mathematical statements, proofs, computer programs, algorithms etc. can be represented by natural numbers.

- Indeed, all finite mathematical objects can be represented using a finite alphabet. We can then code the text with a single natural number.

From now on the sets of numbers we consider are sets of natural numbers.

# Hilbet's program, 1920

David Hilbert 1862–1943

- Russel's paradox (1901): Does the set of all sets that do not belong to themselves belong to itself?
- Can a barber who only shaves people who do not shave themselves shave himself?
- Hilbert's proposal to overcome the paradoxes: Axiomatize all branches of Mathematics so that all true mathematical statements, but no paradoxes/contradictions, can be proved from the axioms.

# Demystyfing algorithms


Muhammad ibn-Musa al-Khwarizmi c. 780 – c. 850

- An algorithm is just a set of instructions —or a kind of " recipe"— to perform a mathematical operation.
- The mathematical operations of multiplication, long division, etc. we learn in high school are examples of algorithms.
- Algorithms as well are the compass and ruler constructions in. geometry.

# How algorithms come into play

- A set of numbers is called

Recursive or decidable if there is an algorithm that given a number outputs YES or NO depending on whether the number belongs to the set or not.

Recursively enumerable (r.e.) if there is an algorithm that lists its elements.

- The fact that there are non-recursive sets of natural numbers might not come as a surprise.
- However the fact that there are r.e. sets that are not recursive is much subtler.

# The thirties and fourties: the golden era of Logic: The refutation of Hilbert's program

Kurt Gödel 1906–1978

- First *Incompleteness Theorem:* No axioms can be found that can prove all true statements.
- *Second Incompleteness Theorem:* No rich enough set of non-contradictory (consistent) axioms can prove their own consistency.

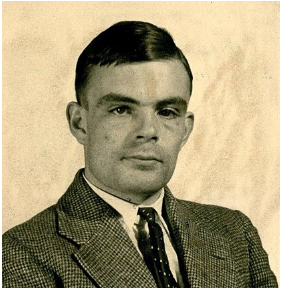
# The golden era of Logic II

Alonzo Church 1903–1995

Undecidability results:

- No algorithm can decide if a statement is provable from the "standard" axioms of Number Theory (Peano Axioms).
- The *Entscheidungsproblem (Decision Problem)* is undecidable, in other words, no algorithm can decide if a logical statement is true independently of how it is interpreted.

# The golden era of Logic III



Alan Turing 1912–1953

- He “designed” the Turing machine, a mathematical model of computing machines, independent of the current level of technology.
- *Church-Turing thesis:* The algorithmically decidable sets are exactly those that a Turing machine can decide.
- *Halting problem:* The problem of whether a Turing machine gives an output on a given input, or enters an infinite loop, is recursively enumerable undecidable (non-recursive).

⋄ The proofs of all these results make strong use of diagonalization (self-referential) arguments, reminiscent of how Cantor proved that real numbers are not countable.

# Diophantine equations

Diophantus of Alexandria
c. 200 – c. 284 CE

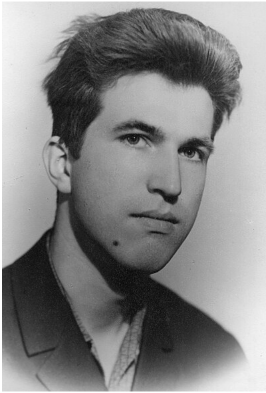
- Known as the *father of Algebra* and famous for his book *Arithmetica*.
- Diophantine Equations: Equations with integer coefficients for which integer solutions are sought.
- Examples: $4x^2 + 3y^2 = 4$ obviously has the only solution $(x = 1, y = 0)$, but $4x + 3y = 4$ has many solutions $((x = 1, y = 0), (x = -2, y = 4), \ldots)$.

# Hilbert's problems

David Hilbert 1862–1943

- Twenty-three problems that were published in 1900. They were unsolved at the time.
- Ten among them were presented at the Paris conference of the International Congress of Mathematicians (1900).
- Only eight of them are generally accepted as being solved today.
- Among the solved ones the tenth problem, H10

# H10 and its negative solution



Yuri Matiyasevich 1947

- H10: Find an algorithm to determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution.
- The set of tuples of integers that are coefficients of solvable Diophantine equations is recursively enumerable.
- Try the first tuple by checking if the first integer is a solution, then try the first two tuples by checking if any of first two integers is a solution ....
- Matiyasevich proved that this set is *not* recursive by representing every r.e. set by a Diophantine equation. Preliminary work by Robinson, Davis, and Putnam.

# H10 for rings and fields

*Ring*: An algebraic structure with a notion of addition, multiplication, and negatives. For example, integers (natural numbers together with their negatives) $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

*Field*: A ring with inverses for non-zeroes. For example the set of rational numbers $\mathbb{Q}$.

Function rings or fields: Functions like polynomials, defined over a ring or a field.

Generalization of H10: Instead of asking if a polynomial with integer coefficient has an integer solution, ask if a polynomial with coefficients in a given ring or field has solutions in that ring or field.

Important open problem: Is H10 over the field of rationals undecidable?

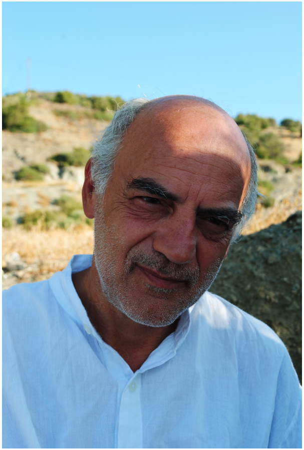
# The ring of complex entire functions

The set of complex numbers $\mathbb{C}$ is the set of numbers of the form $a + ib$ where $a, b$ are real numbers and $i$ is an "imaginary number" whose square is equal to $-1$. $\mathbb{C}$ is a field.

Fundamental theorem of Algebra (19-th century): Every non-zero, single-variable, degree $n$ polynomial with complex coefficients has, counted with multiplicity, exactly $n$ complex roots.

Complex entire functions: Functions that are defined over complex numbers, the values they take are complex numbers, and change smoothly everywhere. They form a ring.

# Thanasis Pheidas

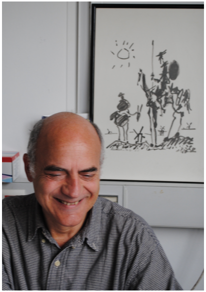


1958–2013

- Thanasis proved the undecidability of H10 for several rings and fields that “come close” to $Q$ or to the ring of entire functions.
- One of his most important results (1991, no co-author): H10 for a field of rational functions in a letter t with coefficients in a finite field of positive characteristic other than 2, is undecidable.
- With X. Vidaux (2017): H10 is undecidable for the ring of complex entire functions in at least 2 variables.

# Thanasis and Number Theory

Carl Friedrich Gauss (1777-1855):
"Mathematics is the queen of the sciences – and number theory is the queen of mathematics."



Pheidas: Important contributions to sequences of natural numbers, like Büchi's problem.

# And a personal note

Friendship survives after loss, when memories are strong.

- Thank you for your attention!