Undecidability in Number Theory

Bjorn Poonen

Presented By

Nandita Krishnan

Existence of Solution

Does the equation $x^3 + y^3 + z^3 = 29$ have a solution in integers?

Existence of Solution

Does the equation $x^3 + y^3 + z^3 = 29$ have a solution in integers?

Yes !

(3,1,1)

Does $x^3 + y^3 + z^3 = 30$ have a solution in integers ?

Existence of Solution

Does the equation $x^3 + y^3 + z^3 = 29$ have a solution in integers?

Yes !

(3,1,1)

Does $x^3 + y^3 + z^3 = 30$ have a solution in integers ?

Yes!

(−283059965, −2218888517, 2220422932)

Does $x^3 + y^3 + z^3 = 33$ have a solution ?

Existence of a Solution?

Not yet !Remains unsolved !

Hence we are interested in the question - Is there an integral solution to a polynomial ?

Brings us back to Hilbert's 10th Problem - H10

Find an algorithm that solves the following problem:

Input: a multivariable polynomial f (x1, . . . , xn) with integer coefficients

Output: YES or NO, according to whether there exist integers a1, a2, . . . , an such that f (a1, . . . , an) = 0.

What is an Algorithm ?

Church-Turing :
Every purely mechanical procedure can be carried out by a Turing machine

Algorithm ≡ Turing machine

Turing machine :

- Finite-length program running on a physical computer containing :
- Unlimited time
- Memory

Few Definitions

DIOPHANTINE

Set $A \subseteq Z$ is diophantine
if there exists a polynomial $p(t, x) \in Z[t, x1, \ldots, xn]$
such that
$A = \{a \in Z : (\exists x \in Z^n)\ p(a, x) = 0\}$.

Example 2. The subset $\mathbb{N} := \{0, 1, 2, \ldots\}$ of $\mathbb{Z}$ is diophantine since for $a \in \mathbb{Z}$, we have

$$a \in \mathbb{N} \iff (\exists x_1, \ldots, x_4 \in \mathbb{Z})\ x_1^2 + \cdots + x_4^2 = a.$$

Few Definitions

LISTABLE

Set A $\subseteq$ Z is listable (or recursively enumerable)
if there is an algorithm that prints A.

Turing machine prints out A ,a set of integers when left running forever.

Obviously any diophantine subset of Z is listable

Few Definitions

COMPUTABLE

Set $A \subseteq Z$ is computable (or recursive) if there is an algorithm for deciding membership in A

Input : Integer a

Outputs:YES or NO ; whether $a \in A$.

The Halting Problem

Determining whether a Turing machine halts
(by accepting or rejecting) on a given input.

Theorem :
The halting problem is undecidable; that is, no Turing machine can solve it.

Corollary : There exists a listable set that is not computable.

THE DPRM THEOREM (Davis,Putnam,Robinson, Matiyasevich 1970)

- A subset of Z is listable if and only if it is diophantine.

To prove their theorem, these four authors :

- Built a computer out of diophantine equations!

- They showed that diophantine equations are rich enough to simulate any computer
- One can construct a polynomial equation that has an integer solution if and only if the program halts.

RESULTS OF H10 PROBLEM :

Undecidability of the halting problem =>There exists a listable set that is not computable.

By the DPRM theorem implies a diophantine set that is not computable.

By definition, this means that we have a polynomial p(t, x) such that there is no algorithm for deciding for which values $a \in Z$ the equation p(a, x) = 0 has a solution in integers x1, . . . , xn.

There cannot be an algorithm for deciding the existence of integer solutions to all polynomial equations.

Fun Consequences of DPRM

- There is an algorithm for a polynomial in one variable any degree to decide the existence of integer solution
- Likely that the problem is decidable for polynomial of degree 2.
- There is an algorithm for equations of degree 1 and 2
- The situation for degree 3 is unknown.
- There is no algorithm for equation of degree 4.

Extended Facts of DPRM Theorem

Even a simple computable equation have smallest solution that is huge

T. Skolem Theorem :
Every higher degree polynomial equation is equivalent to one of degree 4

Reimann Hypothesis

The DPRM theorem gives an explicit polynomial equation that has a solution in integers if and only if the Riemann hypothesis is false.

Sketch of proof.

- Write a computer program that, when left running forever,
- Will detect a counterexample to the Riemann hypothesis if one exists.
- Simulate this program with a DIOPHANTINE equation

H10 over Q (rings)

It is unknown if there exists an algorithm that decides whether a multivariable polynomial equation has a solution in rational numbers.

If Z is diophantine over Q, then the negative answer for Z implies a negative answer for Q.

But there is a conjecture that implies that Z is not diophantine over Q:

First-order sentences over Z

Logic Based Sentences H10 asks for an algorithm to decide the truth of positive existential sentences

$(\exists x1\, \exists x2 \cdots \exists xn)\ p(x1, \ldots, xn) = 0.$
in the language of rings, where the variables run over integers.

To Find an algorithm to decide the truth of arbitrary first-order sentences in which any number of bound quantifiers $\exists$ and $\forall$ are permitted:

First-order sentences over Z

Example of typical such sentence is

$(\exists x)(\forall y)(\exists z)(\exists w)\,(x \cdot z + 3 = y\ 2\ ) \vee \neg(z = x + w)$

Church, G¨odel, and Turing in the 1930

There was no algorithm to solve the harder problem of deciding the truth of first-order sentences over Z.

First-order sentences over Q

It is not known whether Z is diophantine over Q,

Theorem (J. Robinson 1949):

One can characterize Z as the set of $t \in Q$ such that a particular first-order formula of the form $(\forall \sim x)(\exists \sim y)(\forall \sim z)(\exists w\sim)\ p(t,\sim x,\sim y,\sim z,w\sim) = 0$ is true, when the variables range over rational numbers.

Corollary:

There is no algorithm to decide the truth of a first-order sentence over Q

Theorem 18. *The set $\mathbb{Z}$ equals the set of $t \in \mathbb{Q}$ such that*

$$
\begin{aligned}
&(\forall a, b)(\exists x_1, x_2, x_3, x_4, y_2, y_3, y_4) \\
&(a + x_1^2 + x_2^2 + x_3^2 + x_4^2)(b + x_1^2 + x_2^2 + x_3^2 + x_4^2) \\
&\cdot \Big[\left(x_1^2 - a x_2^2 - b x_3^2 + ab x_4^2 - 1 \right)^2 \\
&+ \prod_{n=0}^{2309} \left((n - t - 2x_1)^2 - 4a y_2^2 - 4b y_3^2 + 4ab y_4^2 - 4 \right)^2 \Big] \\
&= 0
\end{aligned}
$$

is true, when the variables range over rational numbers.

H10 over subrings of Q

Let P = {2, 3, 5, . . .}. There is a bijection
{subsets of P} ↔ {subrings of Q}
$S \rightarrow Z[S^{-1}]$.
$Z[S^{-1}]$: Rational Number whose denominator is divisible by prime in S
Examples:
$S = \varnothing$, $Z[S^{-1}] = Z$, answer is negative
Partial Proof 2003 :
There exists a recursive set of primes $S \subset P$ of density 1 such that H10 over $Z[S^{-1}]$ has a negative answer

Status of knowledge

The table below summarizes what is known regarding the questions

- Is there an algorithm for H10 over R?

- Is there an algorithm to decide the truth of arbitrary first-order sentences over R?

Ring	H10	1st order
$\mathbb{C}$	YES	YES
$\mathbb{R}$	YES	YES
$\mathbb{F}_q$	YES	YES
p-adic fields	YES	YES
$\mathbb{F}_q((t))$	?	?
$\overline{\mathbb{Z}}$	YES	YES
number field	?	NO
$\mathbb{Q}$	?	NO
global function field	NO	NO
$\mathbb{F}_q(t)$	NO	NO
$\mathbb{C}(t)$	?	?
$\mathbb{C}(t_1, \ldots, t_n)$, $n \geq 2$	NO	NO
$\mathbb{R}(t)$	NO	NO
$\mathcal{O}_k$	?	NO
$\mathbb{Z}$	NO	NO

REFERENCES

Bjorn Poonen MIT UAM Colloquium March 25, 2010
B. Poonen. Undecidability in number theory. Notices of the Amer. Math. Soc., 55(3):344–350, 2008.
Wikipedia.com

THANK YOU
ANY questions ?