Undecidability in number theory

Bjorn Poonen

Rademacher Lecture 1
November 6, 2017

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 29?$$

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 29?$$

Yes: $(x, y, z) = (3, 1, 1)$.

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 30?$$

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 30?$$

Yes: $(x, y, z) = (-283059965, -2218888517, 2220422932)$.

(discovered in 1999 by E. Pine, K. Yarbrough, W. Tarrant, and M. Beck, following an approach suggested by N. Elkies.)

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 33?$$

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 33?$$

Unknown.

Hilbert's tenth problem

David Hilbert, in the 10th of the list of 23 problems he published after a famous lecture in 1900, asked his audience to find a method that would answer all such questions.

Hilbert's tenth problem (H10)

Find an algorithm that solves the following problem:

input: *a multivariable polynomial* $f(x_1, \ldots, x_n)$ *with integer coefficients*

output: *YES or NO, according to whether there exist integers* $a_1, a_2, \ldots, a_n$ *such that* $f(a_1, \ldots, a_n) = 0$.

More generally, one could ask for an algorithm for solving a system of polynomial equations, but this would be equivalent, since

$$f_1 = \cdots = f_m = 0 \iff f_1^2 + \cdots + f_m^2 = 0.$$

Hilbert's tenth problem

Hilbert's tenth problem (H10)

Find a Turing machine that solves the following problem:

input: *a multivariable polynomial* $f(x_1, \ldots, x_n)$ *with integer coefficients*

output: *YES or NO, according to whether there exist integers* $a_1, a_2, \ldots, a_n$ *such that* $f(a_1, \ldots, a_n) = 0$.

Theorem (Davis–Putnam–Robinson 1961 + Matiyasevich 1970)

No such algorithm exists!

In fact they proved something stronger...

Family of polynomial equations

$$\vdots$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = -2 \qquad \text{NO}$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = -1 \qquad \text{NO}$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0 \qquad \text{YES}$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1 \qquad \text{YES}$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2 \qquad \text{YES}$$

$$\vdots$$

The set of $a \in \mathbb{Z}$ such that

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = a$$

has a solution in integers is

$$\{0, 1, 2, \ldots\} =: \mathbb{N}$$

Family of polynomial equations

$$\vdots$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = -2 \qquad \text{NO}$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = -1 \qquad \text{NO}$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0 \qquad \text{YES}$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1 \qquad \text{YES}$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2 \qquad \text{YES}$$

$$\vdots$$

The set of $a \in \mathbb{Z}$ such that

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 - a = 0$$

has a solution in integers is

$$\{0, 1, 2, \ldots\} =: \mathbb{N}$$

Diophantine sets

Definition

$A \subseteq \mathbb{Z}$ is diophantine if there exists

$$p(t, \vec{x}) \in \mathbb{Z}[t, x_1, \ldots, x_m]$$

such that

$$A = \{\, a \in \mathbb{Z} : p(a, \vec{x}) = 0 \text{ has a solution } \vec{x} \in \mathbb{Z}^m \}.$$

Example

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

$$a \in \mathbb{N} \iff (\exists x_1, x_2, x_3, x_4 \in \mathbb{Z})\; x_1^2 + x_2^2 + x_3^2 + x_4^2 - a = 0.$$

Listable sets

Definition

$A \subseteq \mathbb{Z}$ is listable if there is a Turing machine such that A is the set of integers that it prints out when left running forever.

Example

The set of integers expressible as a sum of three cubes is listable.

(Print out $x^3 + y^3 + z^3$ for all $|x|, |y|, |z| \leq 10$, then print out $x^3 + y^3 + z^3$ for $|x|, |y|, |z| \leq 100$, and so on.)

Halting problem

Can one write a *debugger* to solve the halting problem?

input: program p and natural number x

output: YES if p on input x eventually halts,
NO if it enters an infinite loop.

Theorem (Turing 1936)

No such debugger exists; the halting problem is unsolvable.

Sketch of proof:

Enumerate all programs. If we had a debugger, we could use it to write a new program H such that for every $x \in \mathbb{N}$,

H on input x halts $\iff$ program x on input x does *not* halt.

Taking $x = H$, we find a contradiction:

H on input H halts $\iff$ H on input H does not halt. □

Negative answer to H10

What Davis-Putnam-Robinson-Matiyasevich really proved is:

DPRM theorem: Diophantine $\iff$ listable

(They showed that the theory of diophantine equations is rich enough to simulate any computer!)

The DPRM theorem implies a negative answer to H10:

- The unsolvability of the halting problem provides a listable set for which no algorithm can decide membership.
- So there exists a *diophantine* set for which no algorithm can decide membership.
- Thus H10 has a negative answer.

More fun consequences of the DPRM theorem

"Diophantine $\iff$ listable"
has applications beyond the negative answer to H10:

- Prime-producing polynomials
- Diophantine statement of the Riemann hypothesis

The set of primes equals the set of positive values assumed by the 26-variable polynomial

$$
\begin{gathered}
(k+2)\{1-([wz+h+j-q]^2 \\
+[(gk+2g+k+1)(h+j)+h-z]^2 \\
+[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 \\
+[2n+p+q+z-e]^2+[e^3(e+2)(a+1)^2+1-o^2]^2 \\
+[(a^2-1)y^2+1-x^2]^2+[16r^2y^4(a^2-1)+1-u^2]^2 \\
+[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 \\
+[(a^2-1)\ell^2+1-m^2]^2 \\
+[ai+k+1-\ell-i]^2+[n+\ell+v-y]^2 \\
+[p+\ell(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \\
+[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
+[z+p\ell(a-p)+t(2ap-p^2-1)-pm]^2)\}
\end{gathered}
$$

as the variables range over nonnegative integers (J. Jones, D. Sato, H. Wada, D. Wiens).

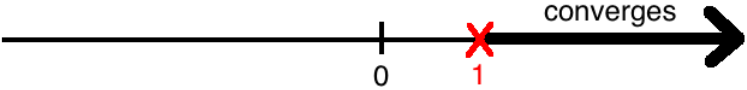
Riemann zeta function

The series

$$\zeta(s) := \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

converges for real numbers $s > 1$.

But $\zeta(s) \to \infty$ as $s \to 1$ from the right.



- Within $\mathbb{R}$, there is no way to extend $\zeta(s)$ to an analytic function across 1 to define it to the left of 1.
- But in $\mathbb{C}$, one can go *around* 1, to get values like

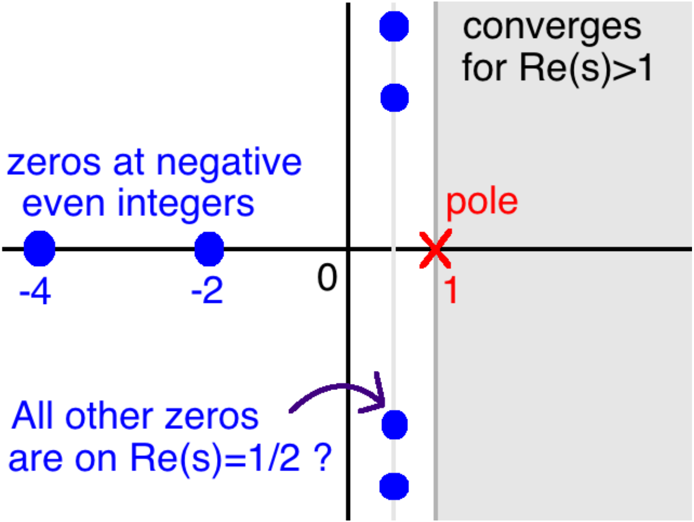
$$\zeta(-1) = -\frac{1}{12}.$$

Some people pretend that this means that

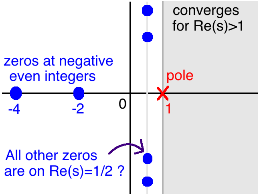
$$1 + 2 + 3 + \cdots = -\frac{1}{12}.$$

Riemann zeta function on the complex plane

$$\zeta(s) := \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots \quad \text{when } \mathrm{Re}(s) > 1.$$



Riemann hypothesis



Riemann hypothesis (from 1859, still not proved)

All zeros of $\zeta(s)$ *except for* $-2, -4, -6, \ldots$ *satisfy* $\mathrm{Re}(s) = 1/2$.

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

Construction of this polynomial equation.

- One can 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 rings of integers

Given a number field k, its ring of integers is

$$\mathcal{O}_k := \{\alpha \in k : f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}.$$

Example

If $k = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, then $\mathcal{O}_k = \mathbb{Z}[i]$.

Conjecture

H10/$\mathcal{O}_k$ has a negative answer for every number field k.

Question

Why can't we just replace $\mathbb{Z}$ by $\mathcal{O}_k$ in the proof of DPRM?

Answer:

- For the Pell equation $T\colon x^2 - dy^2 = 1$ (where $d \in \mathbb{Z}_{>0}$ is a fixed non-square), rank $T(\mathbb{Z}) = 1$.
- For most number fields k, it is impossible to find tori T such that the needed conditions on rank $T(\mathcal{O}_k)$ hold.

On the other hand, there exist other algebraic groups. . .

H10 over rings of integers, continued

Conjecture: Shafarevich–Tate groups of elliptic curves are finite.

$\Downarrow$ Mazur–Rubin 2010

For every prime-degree Galois extension of number fields $L \supseteq K$, there is an elliptic curve E/K with

$$\operatorname{rank} E(L) = \operatorname{rank} E(K) > 0.$$

$\Downarrow$ P., Shlapentokh 2003

For every number field k, H10/$\mathcal{O}_k$ has a negative answer.

Hilbert's tenth problem over $\mathbb{Q}$

Question

Is there an algorithm to decide whether a multivariable polynomial equation has a solution in rational numbers?

The answer is not known!

- If $\mathbb{Z}$ is diophantine over $\mathbb{Q}$, then the negative answer for $\mathbb{Z}$ implies a negative answer for $\mathbb{Q}$.
- But there is a conjecture that implies that $\mathbb{Z}$ is *not* diophantine over $\mathbb{Q}$:

Conjecture (Mazur 1992)

For any polynomial equation $f(x_1, \ldots, x_n) = 0$ with rational coefficients, if S is the set of rational solutions, then the closure of S in $\mathbb{R}^n$ has at most finitely many connected components.

First-order sentences

- H10 is about truth of positive existential sentences

$$(\exists x_1 \exists x_2 \cdots \exists x_n)\ p(x_1, \ldots, x_n) = 0.$$

- Harder problem: Find an algorithm to decide the truth of arbitrary first-order sentences, in which any number of bound quantifiers $\exists$ and $\forall$ are permitted, e.g.,

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

If variables range over integers, this is undecidable (since it is harder than the original H10).

But what if variables range over rational numbers?

Theorem (Robinson 1949, P. 2007, Koenigsmann 2016)

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

$$(\forall a, b)(\exists x_1, x_2, x_3, x_4, y_2, y_3, y_4)$$
$$(a + x_1^2 + x_2^2 + x_3^2 + x_4^2)(b + x_1^2 + x_2^2 + x_3^2 + x_4^2)$$
$$\cdot \Big[\big(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1\big)^2$$
$$+ \big((t - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4\big)^2 \Big] = 0$$

is true, when the variables range over rational numbers.

Corollary (Robinson 1949)

There is no algorithm to decide the truth of a first-order sentence over $\mathbb{Q}$.

Building on these ideas, Koenigsmann (2016) proved also that the *complement* $\mathbb{Q} - \mathbb{Z}$ is diophantine over $\mathbb{Q}$.
This was generalized to number fields by Jennifer Park.

Subrings of $\mathbb{Q}$

There are rings between $\mathbb{Z}$ and $\mathbb{Q}$:

Example

$$\mathbb{Z}[1/2] := \left\{ \frac{a}{2^m} : a \in \mathbb{Z},\ m \geq 0 \right\}$$

Example

$$\mathbb{Z}[1/2, 1/3] := \left\{ \frac{a}{2^m 3^n} : a \in \mathbb{Z},\ m, n \geq 0 \right\}$$

In general, if $S \subseteq \mathcal{P} := \{\text{all primes}\}$, one can define

$$\begin{aligned} \mathbb{Z}[S^{-1}] &= \text{the subring of } \mathbb{Q} \text{ generated by } p^{-1} \text{ for all } p \in S \\ &= \left\{ \frac{a}{d} : a \in \mathbb{Z},\ d \text{ is a product of powers of primes in } S \right\} \end{aligned}$$

Proposition

Every subring of $\mathbb{Q}$ is of the form $\mathbb{Z}[S^{-1}]$ for a unique S.

H10 over subrings of $\mathbb{Q}$

Proposition

Every subring of $\mathbb{Q}$ is of the form $\mathbb{Z}[S^{-1}]$ for a unique S.

Examples:

- $S = \emptyset$, $\mathbb{Z}[S^{-1}] = \mathbb{Z}$, *answer is negative.*
- $S = \mathcal{P}$, $\mathbb{Z}[S^{-1}] = \mathbb{Q}$, *answer is unknown.*

- How large can we make S (in the sense of density) and still prove a negative answer for H10 over $\mathbb{Z}[S^{-1}]$?
- For finite S, a negative answer follows from work of Robinson, who used the Hasse-Minkowski theorem (local-global principle) for quadratic forms.

H10 over subrings of $\mathbb{Q}$, continued

Theorem (P., 2003)

There exists a computable set of primes $S \subset \mathcal{P}$ of density 1 such that H10 over $\mathbb{Z}[S^{-1}]$ has a negative answer.

The proof use properties of integral points on elliptic curves.

Ring	H10	1st order theory
$\mathbb{C}$	YES	YES
$\mathbb{R}$	YES	YES
$\mathbb{F}_q$	YES	YES
p-adic fields	YES	YES
$\mathbb{F}_q((t))$	?	?
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

increasing arithmetic complexity →