Hilbert's Tenth Problem

Bjorn Poonen

University of California at Berkeley

MSRI Introductory Workshop on Rational and Integral Points on Higher-dimensional Varieties

January 18, 2006

The original problem

H10: Find an algorithm that solves the following problem:

input: $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$
output: *YES or NO, according to whether there exists $\vec{a} \in \mathbb{Z}^n$ with $f(\vec{a}) = 0$.*

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

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

Theorem (Davis-Putnam-Robinson 1961 + Matijasevič 1970)

No such algorithm exists.

In fact they proved something stronger...

Diophantine, listable, recursive sets

- $A \subseteq \mathbb{Z}$ is called diophantine if there exists
$$p(t, \vec{x}) \in \mathbb{Z}[t, x_1, \ldots, x_m]$$
such that
$$A = \{\, a \in \mathbb{Z} : (\exists \vec{x} \in \mathbb{Z}^m)\; p(a, \vec{x}) = 0 \,\}.$$
Example: The subset $\mathbb{N} := \{0, 1, 2, \ldots\}$ of $\mathbb{Z}$ is diophantine, since for $a \in \mathbb{Z}$,
$$a \in \mathbb{N} \iff (\exists x_1, x_2, x_3, x_4 \in \mathbb{Z})\; x_1^2 + x_2^2 + x_3^2 + x_4^2 = a.$$
- $A \subseteq \mathbb{Z}$ is listable (recursively enumerable) if there is a Turing machine such that A is the set of integers that it prints out when left running forever.
- $A \subseteq \mathbb{Z}$ is recursive if there is an algorithm for deciding membership in A:

input: $a \in \mathbb{Z}$
output: *YES if $a \in A$, NO otherwise*

Negative answer

- Recursive $\implies$ listable: A computer program can loop through all integers $a \in \mathbb{Z}$, and check each one for membership in A, printing YES if so.
- Diophantine $\implies$ listable: A computer program can loop through all $(a, \vec{x}) \in \mathbb{Z}^{1+m}$ and print out a if $p(a, \vec{x}) = 0$.
- Listable $\not\Longrightarrow$ recursive: This is equivalent to the undecidability of the Halting Problem of computer science.
- Listable $\implies$ diophantine: This is what Davis-Putnam-Robinson-Matijasevič really proved.

Corollary (negative answer to H10)

There exists a diophantine set that is not recursive. In other words, there is a polynomial equation depending on a parameter for which no algorithm can decide for which values of the parameter the equation has a solution.

Generalizing H10 to other rings

Let R be a ring (commutative, associative, with 1).

H10/R: Is there an algorithm with

input: $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$
output: *YES or NO, according to whether there exists $\vec{a} \in R^n$ with $f(\vec{a}) = 0$?*

Technicality:

- The question presumes that an encoding of the elements of R suitable for input into a Turing machine has been fixed.
- For many R, there exist several obvious encodings and it does not matter which one we select, because algorithms exist for converting from one encoding to another.
- For other rings (e.g. uncountable rings like $\mathbb{C}$), one should restrict the input to polynomials with coefficients in a subring R_0 (like $\overline{\mathbb{Q}}$) whose elements admit an encoding.

Examples of H10 over other rings

$\mathbb{Z}$: NO by D.-P.-R.-Matijasevič

$\mathbb{C}$: YES, by elimination theory

$\mathbb{R}$: YES, by Tarski's elimination theory for semialgebraic sets (sets defined by polynomial equations and inequalities)

$\mathbb{Q}_p$: YES, again because of an elimination theory

$\mathbb{F}_q$: YES, trivially!

In the last four examples, there is even an algorithm for the following more general problem:

input: *First order sentence in the language of rings, such as*

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

output: *YES or NO, according to whether it holds when the variables are considered to run over elements of R*

H10 over rings of integers

k : *number field (finite extension of $\mathbb{Q}$).*

$\mathcal{O}_k$: *the ring of integers of k (the set of $\alpha \in k$ such that $p(\alpha) = 0$ for some monic $p \in \mathbb{Z}[x]$)*

Examples:

- $k = \mathbb{Q}, \quad \mathcal{O}_k = \mathbb{Z}$
- $k = \mathbb{Q}(i), \quad \mathcal{O}_k = \mathbb{Z}[i]$
- $k = \mathbb{Q}(\sqrt{5}), \quad \mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Conjecture

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

H10 over rings of integers, continued

- The negative answer for $\mathbb{Z}$ used properties of the Pell equation $x^2 - dy^2 = 1$ (where $d \in \mathbb{Z}_{>0}$ is a fixed non-square). Its integer solutions form a finitely generated abelian group related to $\mathcal{O}^*_{\mathbb{Q}(\sqrt{d})}$.
- The same ideas give a negative answer for H10/$\mathcal{O}_k$, provided that certain conditions on the rank of groups like this (integral points on tori) are satisfied. But they are satisfied only for special k, such as totally real k and a few other classes of number fields.

Theorem (P., Shlapentokh 2003)

If there is an elliptic curve $E/\mathbb{Q}$ with

$$\operatorname{rank} E(k) = \operatorname{rank} E(\mathbb{Q}) > 0,$$

then H10/$\mathcal{O}_k$ has a negative answer.

H10 over $\mathbb{Q}$

H10/$\mathbb{Q}$ is equivalent to the existence of an algorithm for deciding whether an algebraic variety over $\mathbb{Q}$ has a rational point.

Does the negative answer for H10/$\mathbb{Z}$ imply a negative answer for H10/$\mathbb{Q}$?

- Given a polynomial system over $\mathbb{Q}$, one can construct a polynomial system over $\mathbb{Z}$ that has a solution (over $\mathbb{Z}$) if and only if the original system has a solution over $\mathbb{Q}$: namely, replace each original variable by a ratio of variables, clear denominators, and add additional equations that imply that the denominator variables are nonzero.
- Thus H10/$\mathbb{Q}$ is embedded as a subproblem of H10/$\mathbb{Z}$.
- Unfortunately, this goes the wrong way, if we are trying to use the non-existence of an algorithm for H10/$\mathbb{Z}$ to deduce the non-existence of an algorithm for H10/$\mathbb{Q}$.

Conjectural approaches to H10 over $\mathbb{Q}$

- If the subset $\mathbb{Z} \subseteq \mathbb{Q}$ were diophantine/$\mathbb{Q}$, then we could deduce a negative answer for H10/$\mathbb{Q}$.
  (*Proof:* If there were an algorithm for $\mathbb{Q}$, then to solve an equation over $\mathbb{Z}$, consider the same equation over $\mathbb{Q}$ with auxiliary equations saying that the rational variables take integer values.)
- More generally, it would suffice to have a diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$: a diophantine subset $A \subseteq \mathbb{Q}^m$ equipped with a bijection $\phi\colon A \to \mathbb{Z}$ such that the graphs of addition and multiplication (subsets of $\mathbb{Z}^3$) correspond to diophantine subsets of $A^3 \subseteq \mathbb{Q}^{3m}$.

It is not known whether $\mathbb{Z}$ is diophantine over $\mathbb{Q}$, or whether a diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ exists. (Can $E(\mathbb{Q})$ for an elliptic curve of rank 1 serve as a diophantine model?)

Rational points in the real topology

If X is a variety over $\mathbb{Q}$, then $X(\mathbb{Q})$ is a subset of $X(\mathbb{R})$, and $X(\mathbb{R})$ has a topology coming from the topology of $\mathbb{R}$.

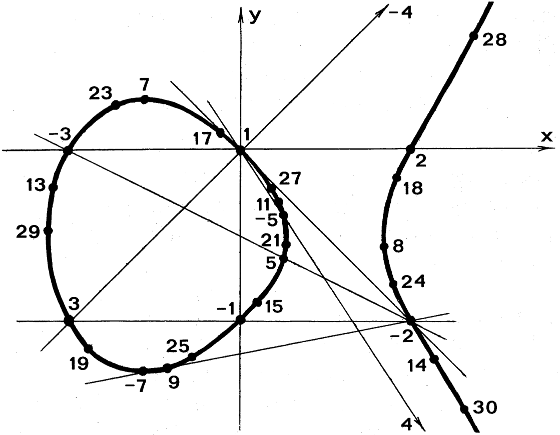


Figure 17. Rational points on the curve $y^2 + y = x^3 - x$.

(The figure is from Hartshorne, *Algebraic geometry*.)

Mazur's conjecture

Conjecture (Mazur 1992)

The closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has at most finitely many connected components.

- This conjecture is true for curves.
- There is very little evidence for or against the conjecture in the higher-dimensional case.

The next two frames will discuss the connection between Mazur's conjecture and H10/$\mathbb{Q}$.

Proposition

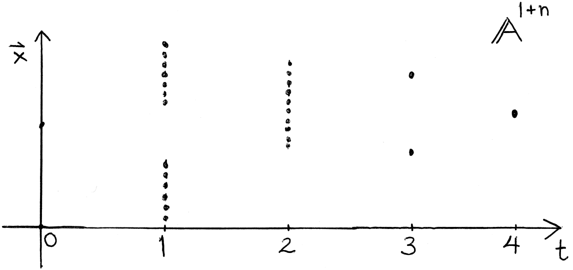
If $\mathbb{Z}$ is diophantine over $\mathbb{Q}$, then Mazur's conjecture is false.

Proof.

Suppose $\mathbb{Z}$ is diophantine over $\mathbb{Q}$; this means that there exists a polynomial $p(t, \vec{x})$ such that

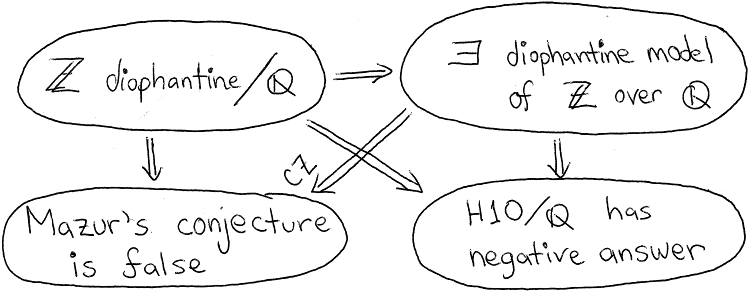
$$\mathbb{Z} = \{a \in \mathbb{Q} : (\exists \vec{x} \in \mathbb{Q}^m)\ p(a, \vec{x}) = 0\}.$$

Let X be the variety $p(t, \vec{x}) = 0$ in $\mathbb{A}^{1+n}$. Then $\overline{X(\mathbb{Q})}$ has infinitely many components, at least one above each $t \in \mathbb{Z}$. $\square$



Mazur's conjecture and diophantine models

- We just showed that Mazur's conjecture is incompatible with the statement that $\mathbb{Z}$ is diophantine over $\mathbb{Q}$.
- Cornelissen and Zahidi have shown that Mazur's conjecture is incompatible also with the existence of a diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.



H10 over subrings of $\mathbb{Q}$

Let $\mathcal{P} = \{2, 3, 5, \ldots\}$. There is a bijection

$$\{\text{subsets of } \mathcal{P}\} \leftrightarrow \{\text{subrings of } \mathbb{Q}\}$$
$$S \mapsto \mathbb{Z}[S^{-1}].$$

Examples:

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

- What happens for S in between?
- 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 recursive set of primes $S \subset \mathcal{P}$ of density 1 such that

1. *There exists a curve E such that $E(\mathbb{Z}[S^{-1}])$ is an infinite discrete subset of $E(\mathbb{R})$. (So the analogue of Mazur's conjecture for $\mathbb{Z}[S^{-1}]$ is false.)*
2. *There is a diophantine model of $\mathbb{Z}$ over $\mathbb{Z}[S^{-1}]$.*
3. *H10 over $\mathbb{Z}[S^{-1}]$ has a negative answer.*

The proof takes E to be an elliptic curve (minus ∞), and uses 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