Hilbert's Tenth Problem, Mazur's Conjectures and Poonen's Theorem

Alexandra Shlapentokh

East Carolina University

Arithmetic of Fields, Oberwolfach
February, 2006

Table of Contents

Hilbert's Question about Polynomial Equations

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers?

Using modern terms one can ask if there exists a program taking coefficients of a polynomial equation as input and producing "yes" or "no" answer to the question "Are there integer solutions?".

This problem became known as Hilbert's Tenth Problem

The Answer

This question was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matijasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine subsets of $\mathbb{Z}$.

Recursive and Recursively Enumerable Subsets of $\mathbb{Z}$

Recursive Sets

A set $A \subseteq \mathbb{Z}$ is called recursive or decidable if there is an algorithm (or a computer program) to determine the membership in the set.

Recursively Enumerable Sets

A set $A \subseteq \mathbb{Z}$ is called recursively enumerable if there is an algorithm (or a computer program) to list the set.

Theorem

There exist recursively enumerable sets which are not recursive.

Diophantine Sets

Diophantine Sets

A subset $A \subset \mathbb{Z}$ is called Diophantine over $\mathbb{Z}$ if there exists a polynomial $p(T, X_1, \ldots, X_k)$ with rational integer coefficients such that for any element $t \in \mathbb{Z}$ we have that

$$(\exists x_1, \ldots, x_k \in \mathbb{Z} : p(t, x_1, \ldots, x_k) = 0) \Longleftrightarrow t \in A.$$

In this case we call $p(T, X_1, \ldots, X_k)$ a Diophantine definition of A over $\mathbb{Z}$.

Corollary

There are undecidable Diophantine subsets of $\mathbb{Z}$.

Intersections and Unions of Diophantine Sets

Lemma

Intersections and unions of Diophantine sets are Diophantine.

Proof.

Suppose $P_1(T, \bar{X}), P_2(T, \bar{Y})$ are Diophantine definitions of subsets A_1 and A_2 of $\mathbb{Z}$ respectively over $\mathbb{Z}$. Then

$$P_1(T, \bar{X})P_2(T, \bar{Y})$$

is a Diophantine definition of $A_1 \cup A_2$, and

$$P_1^2(T, \bar{X}) + P_2^2(T, \bar{Y})$$

is a Diophantine definition of $A_1 \cap A_2$. □

One vs. Finitely Many

Replacing Finitely Many by One

- We can let Diophantine definitions consist of several equations without changing the nature of the relation.
- Any finite system of equations over $\mathbb{Z}$ can be effectively replaced by a single polynomial equation over $\mathbb{Z}$ with the identical $\mathbb{Z}$-solution set.
- The statements above remain valid if we replace $\mathbb{Z}$ by any recursive integral domain R whose fraction field is not algebraically closed.

A General Question

A Question about an Arbitrary Recursive Ring R

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in R, can determine whether this equation has solutions in R?

This question is still open for $R = \mathbb{Q}$ and R equal to the ring of integers of an arbitrary number field.

Note that undecidability of HTP over $\mathbb{Q}$ would imply the undecidability of HTP over $\mathbb{Z}$, but the reverse implication does not hold.

Using Diophantine Definitions to Solve the Problem

Lemma

Let R be a recursive ring of characteristic 0 such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over R. Then HTP is not decidable over R.

Proof.

Let $h(T_1, \ldots, T_l)$ be a polynomial with rational integer coefficients and consider the following system of equations.

$$\begin{cases} h(T_1, \ldots, T_l) = 0 \\ p(T_1, \bar{X}_1) = 0 \\ \ldots \\ p(T_l, \bar{X}_l) = 0 \end{cases} \quad (1)$$

It is easy to see that $h(T_1, \ldots, T_l) = 0$ has solutions in $\mathbb{Z}$ iff (1) has solutions in R. Thus if HTP is decidable over R, it is decidable over $\mathbb{Z}$. □

The Plan

So to show that HTP is undecidable over $\mathbb{Q}$ we just need to construct a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$!!!

The Statement of Conjectures

The Conjecture on the Topology of Rational Points

Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

Corollary

There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

Another Plan: Diophantine Models

What is a Diophantine Model?

Let R be a recursive ring and let $\phi : \mathbb{Z} \longrightarrow R$ be a recursive injection mapping Diophantine sets of $\mathbb{Z}$ to Diophantine sets of R. Then ϕ is called a Diophantine model of $\mathbb{Z}$ over R.

Remarks

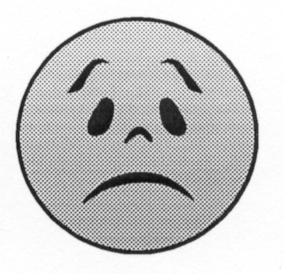
- It is enough to require that the ϕ-images of the graphs of $\mathbb{Z}$-addition and $\mathbb{Z}$-multiplication are Diophantine over R.
- If R has a Diophantine model of $\mathbb{Z}$, then R has undecidable Diophantine sets.

So all we need is a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$!!!!

A Theorem of Cornelissen and Zahidi

Theorem

If Mazur's conjecture on topology of rational points holds, then there is no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.



The Rings between $\mathbb{Z}$ and $\mathbb{Q}$

A Ring in between

Let $\mathcal{S}$ be a set of (non-archimedean) primes of $\mathbb{Q}$. Let $O_{\mathbb{Q},\mathcal{S}}$ be the following subring of $\mathbb{Q}$.

$$\{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, n \text{ is divisible by primes of } \mathcal{S} \text{ only } \}$$

If $\mathcal{S} = \emptyset$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Z}$. If $\mathcal{S}$ contains all the primes of $\mathbb{Q}$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Q}$. If $\mathcal{S}$ is finite, we call the ring small. If $\mathcal{S}$ is infinite, we call the ring large.

Small Subrings of Number Fields

Theorem

Let K be a number field. Let $\mathfrak{p}$ be a non-archimedean prime of K. Then the set of elements of K integral at $\mathfrak{p}$ is Diophantine over K. (Julia Robinson and others)

Theorem

Let K be a number field. Let $\mathcal{S}$ be any set of non-archimedean primes of K. Then the set of non-zero elements of $O_{K,\mathcal{S}}$ is Diophantine over $O_{K,\mathcal{S}}$. (Denef, Lipshitz)

Corollary

- *$\mathbb{Z}$ has a Diophantine definition over the small subrings of $\mathbb{Q}$.*
- *HTP is undecidable over the small subrings of $\mathbb{Q}$.*

Large Subrings of Number Fields

Theorem

Let K be a totally real number field or an extension of degree 2 of a totally real number field, and let $\varepsilon > 0$ be given. Then there exists a set $\mathcal{S}$ of non-archimedean primes of K such that

- *The natural density of $\mathcal{S}$ is greater $1 - \frac{1}{[K:\mathbb{Q}]} - \varepsilon$.*
- *$\mathbb{Z}$ is a Diophantine subset of $O_{K,\mathcal{S}}$.*
- *HTP is undecidable over $O_{K,\mathcal{S}}$.*

Note that this result says nothing about subrings of $\mathbb{Q}$.

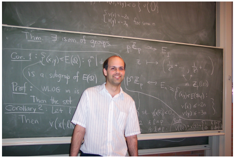
Ring Version of Mazur's Conjecture

An Easier Question?

Let K be a number field and let $\mathcal{W}$ be a set of non-archimedean primes of K. Let V be any affine algebraic set defined over K. Let $\overline{V(O_{K,\mathcal{W}})}$ be the topological closure of $V(O_{K,\mathcal{W}})$ in $\mathbb{R}$ if $K \subset \mathbb{R}$ or in $\mathbb{C}$, otherwise. Then how many connected components does $\overline{V(O_{K,\mathcal{W}})}$ have?

The ring version of Mazur's conjecture has the same implication for Diophantine definability and models as its field counterpart.

The Statement of Poonen's Theorem



Theorem

There exist recursive sets of rational primes $\mathcal{T}_1$ and $\mathcal{T}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of rational primes containing $\mathcal{T}_1$ and avoiding $\mathcal{T}_2$, the following hold:

- *There exists an affine curve E defined over $\mathbb{Q}$ such that the topological closure of $E(O_{\mathbb{Q},\mathcal{S}})$ in $E(\mathbb{R})$ is an infinite discrete set. Thus the ring version of Mazur's conjecture does not hold for $O_{\mathbb{Q},\mathcal{S}}$.*
- *$\mathbb{Z}$ has a Diophantine model over $O_{\mathbb{Q},\mathcal{S}}$.*
- *Hilbert's Tenth Problem is undecidable over $O_{\mathbb{Q},\mathcal{S}}$.*

A Proof Overview

The proof of the theorem relies on the existence of an elliptic curve E defined over $\mathbb{Q}$ such that the following conditions are satisfied.

- $E(\mathbb{Q})$ is of rank 1. (For the purposes of our discussion we will assume the torsion group is trivial.)
- $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ as topological groups.
- E does not have complex multiplication.

Proof Steps

Fix an affine Weierstrass equation for E of the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

1. Show that there exists a computable sequence of rational primes $l_1 < \ldots < l_n < \ldots$ such that $[l_j]P = (x_{l_j}, y_{l_j})$, and for all $j \in \mathbb{Z}_{>0}$, we have that $|y_{l_j} - j| < 10^{-j}$.
2. Prove the existence of infinite sets $\mathcal{T}_1$ and $\mathcal{T}_2$, as described in the statement of the theorem, such that for any set $\mathcal{S}$ of rational primes containing $\mathcal{T}_1$ and disjoint from $\mathcal{T}_2$, we have that

$$E(O_{\mathbb{Q},\mathcal{S}}) = \{[\pm l_j]P\} \cup \{\text{ finite set }\}.$$

3. Note that $\{y_{l_j}\}$ is an infinite discrete Diophantine set over the ring in question, and thus is a counterexample to Mazur's conjecture for the ring $O_{\mathbb{Q},\mathcal{S}}$.
4. Show that $\{y_{l_j}\}$ is a Diophantine model of $\mathbb{Z}_{>0}$ over $\mathbb{Q}$.

Constructing a Model of $\mathbb{Z}_{>0}$ using y_{l_j}'s, I

We claim that $\phi : j \longrightarrow y_{l_j}$ is a Diophantine model of $\mathbb{Z}_{>0}$. In other words we claim that ϕ is a recursive injection and the following sets are Diophantine:

$$D+ = \{(y_{l_i}, y_{l_j}, y_{l_k}) \in D^3 : k = i + j, k, i, j \in \mathbb{Z}_{>0}\}$$

and

$$D_2 = \{(y_{l_i}, y_{l_k}) \in D^2 : k = i^2, i \in \mathbb{Z}_{>0}\}.$$

(Note that if $D+$ and D_2 are Diophantine, then $D_\times = \{(y_{l_i}, y_{l_j}, y_{l_k}) \in D^3 : k = ij, k, i, j \in \mathbb{Z}_{>0}\}$ is also Diophantine since $xy = \frac{1}{2}((x+y)^2 - x^2 - y^2.)$

Constructing a Model of $\mathbb{Z}_{>0}$ Using y_{l_j}'s, II

Theorem

The set positive numbers is Diophantine over $\mathbb{Q}$. (Legendre)

Sums and Squares Are Diophantine

It is easy to show that

$$k = i + j \Leftrightarrow |y_{l_i} + y_{l_j} - y_{l_k}| < 1/3.$$

and with the help of Legendre this makes D_+ Diophantine. Similarly we have that

$$k = i^2 \Leftrightarrow |y_{l_i}^2 - y_{l_k}| < 2/5,$$

implying that D_2 is Diophantine.

Arranging to Get Close to Positive Integers

The fact that for any $\{\varepsilon_j\} \subset \mathbb{R}_{>0}$, we can construct a prime sequence $\{l_j\}$ with $|y_{l_j} - j| < \varepsilon_j$ follows from a result of Vinogradov.

Theorem

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Let $J \subseteq [0, 1]$ be an interval. Then the natural density of the set of primes

$$\{l \in \mathcal{P}(\mathbb{Q}) : (l\alpha \mod 1) \in J\}$$

is equal to the length of J.

From this theorem we obtain the following corollary.

Corollary

Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ as topological groups. Let P be any point of infinite order. Then for any interval $J \subset \mathbb{R}$ whose interior is non-empty, the set $\{l \in \mathcal{P}(\mathbb{Q}) | y([l]P) \in J\}$ has positive natural density.

Getting Rid of Undesirable Points.

The primes in the denominator.

The next issue which needs to be considered is selecting primes for $\mathcal{S}$ so that $E(O_{\mathbb{Q},\mathcal{S}})$ essentially consists of $\{[\pm l_j]P, j \in \mathbb{Z}_{>0}\}$. This part depends on the following key facts.

- Let p be a rational prime outside a finite set of primes which depends on the choice of the curve and the Weierstrass equation. Then for non-zero integers m, n such that $m|n$, if p occurs in the reduced denominators of $(x_m, y_m) = [m]P$, then p occurs in the reduced denominators of $(x_n, y_n) = [n]P$.
- If m, n are as above and are large enough with $n > m$, then there exists a prime q which occurs in the reduced denomiantors of (x_n, y_n) but not in the reduced denominators of (x_m, y_m).
- If $(m, n) = 1$ then the set of primes which can occur in both denominators of any corresponding pairs is finite.

The Messy Part

The most difficult part of the proof is making sure that the sets of primes we have to remove and have to keep are of natural density 0.

For a prime ℓ let p_ℓ be the largest prime dividing the reduced denominators of $(x_\ell, y_\ell) = [\ell]P$. The challenging part here is showing that the set

$$\{p_\ell : \ell \in \mathcal{P}(\mathbb{Q})\}$$

is of natural density 0. One of the required tools is Serre's result on the action of the absolute Galois group on the torsion points of the elliptic curve.

The Source

"Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$", Journal of American Mathematical Society, volume 16 (2003), no. 4, 981–990.

Hilbert's Tenth Problem:
Diophantine Classes and Extensions to Global Fields
Series: New Mathematical Monographs (No. 7)
Alexandra Shlapentokh
East Carolina University
Hardback
(ISBN-10: 0521833604 | ISBN-13: 9780521833608)
Not yet published - available from June 2006 c. $95.00 (C)