All Things Diophantine: Diophantine Stability and Diophantine Definability

Alexandra Shlapentokh

East Carolina University,
Greenville, North Carolina, USA

Oberwolfach Workshop on Computability, January 2018

East Carolina UNIVERSITY

Outline

East Carolina University

The Origin

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

East Carolina University

An answer to Hilbert's Question

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 Matiyasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine sets.

East Carolina UNIVERSITY

Diophantine Sets: a Number-Theoretic Definition

For an integral domain R, a subset $A \subset R^m$ is called Diophantine over R if there exists a polynomial $p(T_1, \ldots T_m, X_1, \ldots, X_k)$ with coefficients in R such that for any element $(t_1, \ldots, t_m) \in R^m$ we have that

$$\exists x_1, \ldots, x_k \in R : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of A over R.

East Carolina University

Diophantine Sets: a Number-Theoretic Definition

For an integral domain R, a subset $A \subset R^m$ is called Diophantine over R if there exists a polynomial $p(T_1, \ldots T_m, X_1, \ldots, X_k)$ with coefficients in R such that for any element $(t_1, \ldots, t_m) \in R^m$ we have that

$$\exists x_1, \ldots, x_k \in R : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of A over R.

Remark

Diophantine sets can also be described as the sets existentially definable in the language of rings or as projections of algebraic sets.

East Carolina UNIVERSITY

Undecidable Diophantine Sets

Theorem (MDRP)

There are undecidable Diophantine sets over $\mathbb{Z}$.

East Carolina University

Undecidable Diophantine Sets

Theorem (MDRP)

There are undecidable Diophantine sets over $\mathbb{Z}$.

Corollary

HTP is undecidable or positive existential theory of $\mathbb{Z}$ is undecidable.

East Carolina UNIVERSITY

Undecidable Diophantine Sets

Theorem (MDRP)

There are undecidable Diophantine sets over $\mathbb{Z}$.

Corollary

HTP is undecidable or positive existential theory of $\mathbb{Z}$ is undecidable.

Proof.

Let $f(t, \bar{x})$ be a Diophantine definition of an undecidable Diophantine set. If HTP is decidable, then for each $t \in \mathbb{Z}$ we can determine if the polynomial equation $f(t, \bar{x}) = 0$ has solutions in $\mathbb{Z}$. However, this process would also determine whether t is an element of our set, contradicting the fact that the set was undecidable. □

East Carolina UNIVERSITY

Some Properties of Diophantine Sets and Definitions over Subrings (of Algebraic Extensions) of $\mathbb{Q}$

- Intersections and unions of Diophantine sets are Diophantine (unions always, intersection over not algebraically closed fields).

East Carolina UNIVERSITY

Some Properties of Diophantine Sets and Definitions over Subrings (of Algebraic Extensions) of $\mathbb{Q}$

- Intersections and unions of Diophantine sets are Diophantine (unions always, intersection over not algebraically closed fields).
- One = finitely many (not algebraically closed fields)

East Carolina University

Some Properties of Diophantine Sets and Definitions over Subrings (of Algebraic Extensions) of $\mathbb{Q}$

- Intersections and unions of Diophantine sets are Diophantine (unions always, intersection over not algebraically closed fields).
- One = finitely many (not algebraically closed fields)
- The set of non-zero elements is Diophantine (over all integrally closed subrings).

East Carolina UNIVERSITY

Outline

East Carolina UNIVERSITY

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?

East Carolina University

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?

The most prominent open questions are probably the decidability of HTP for $R = \mathbb{Q}$ and R equal to the ring of integers of an arbitrary number field.

East Carolina University

Using Diophantine Definitions to Solve the Problem

Lemma

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

East Carolina UNIVERSITY

Using Diophantine Definitions to Solve the Problem

Lemma

Let R be a recursive ring containing $\mathbb{Z}$ and 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.

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

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 $\mathbb{Z}$. □

Outline

East Carolina UNIVERSITY

Number fields and Rings of Integers of Number Fields

- A number field is a finite extension of $\mathbb{Q}$.
- An algebraic integer is a root of a monic irreducible polynomial over $\mathbb{Z}$.
- All algebraic integers contained in a number field K form a subring O_K of K called the ring of integers of K.
- Alternatively, the ring of integers of K is the integral closure of $\mathbb{Z}$ in K.

East Carolina UNIVERSITY

What we know.

Theorem

The ring $\mathbb{Z}$ has a diophantine definition and Hilbert's Tenth Problem is undecidable over the rings of integers of the following fields:

- *Extensions of degree 4 that are not totally real and containing a subfield K such that $[K : \mathbb{Q}] = 2$; or totally real number fields and their extensions of degree 2. (Denef 80, Denef and Lipshitz 78) These fields include all Abelian extensions.*
- *Number fields with exactly one pair of non-real embeddings (Pheidas 88, S. 89)*
- *Any number field K such that there exists an elliptic curve E of positive rank defined over $\mathbb{Q}$ with $[E(K) : E(\mathbb{Q})] < \infty$. (Poonen 02 and S. 08)*
- *Any number field K such that there exists an elliptic curve of rank 1 over K and an Abelian variety of positive rank over $\mathbb{Q}$ keeping its rank over K. (Cornilessen, Pheidas, Zahidi 05)*

Cyclic extensions of prime degree are enough

Proposition (Diophantine Stability for Cyclic Extensions of Prime Degree)

If for any pair of number fields M and K such that M/K is a cyclic extension of prime degree there exists an elliptic curve E defined over K such that $\operatorname{rank} E(M) = \operatorname{rank} E(K) > 0$, *then $\mathbb{Z}$ is existentially definable over the ring of integers of any number field and therefore HTP is unsolvable over the ring of integers of any number field.*

East Carolina UNIVERSITY

Cyclic extensions of prime degree are enough

Proposition (Diophantine Stability for Cyclic Extensions of Prime Degree)

If for any pair of number fields M and K such that M/K is a cyclic extension of prime degree there exists an elliptic curve E defined over K such that $\operatorname{rank} E(M) = \operatorname{rank} E(K) > 0$, *then $\mathbb{Z}$ is existentially definable over the ring of integers of any number field and therefore HTP is unsolvable over the ring of integers of any number field.*

- Diophantine Stability for Cyclic Extensions of Prime Degree follows from a part of Shafarevich-Tate (Mazur, Rubin 10)
- Diophantine Stability for Cyclic Extensions of Prime Degree follows from the rank part of BSD and the automorphy conjecture (Murty, Pasten 16)

East Carolina UNIVERSITY

A sequence of simple reductions

Proposition

If $K - L - M$ is an extension of number fields and O_K is Diophantine over O_M, then O_K is Diophantine over O_L. Therefore without loss of generality we can assume that all field extensions under consideration are Galois.

Proof.

Consider the extension $K \longrightarrow L \longrightarrow M$. Let $\Omega = \{1, \ldots, \alpha^{n-1}\} \subset O_M$ be an integral basis of M over L, and let $P(T, \bar{X})$ be a Diophantine definition of O_K over O_M. Then $P(T, \sum_{i=0}^{n-1} X_{1,j}\alpha^j, \ldots, \sum_{i=0}^{n-1} X_{m,j}\alpha^j)$, rewritten so that all occurrences of α are eliminated, is a Diophantine definition of $\mathbb{Z}$ over K. □

East Carolina UNIVERSITY

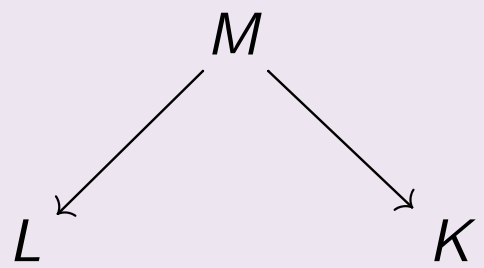
More reductions

Proposition

If M is a number field containing number fields K and L such that O_K and O_L are both Diophantine over O_M. Then $O_K \cap O_L$ is Diophantine over O_M.

Proof.

Consider the following field diagram:



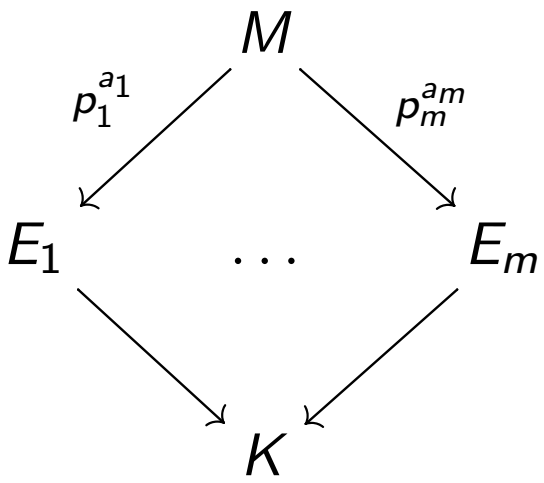
The following system of equations has solutions in O_M if and only if $T \in O_M$:

$$\begin{cases} P_K(T, \bar{X}) = 0 \\ P_L(T, \bar{Y}) = 0 \end{cases}$$

Here P_L, P_K are Diophantine definitions of O_L and O_K respectively over O_M. □

Using Cyclic Extension

Let M/K be a Galois extension. Let $E_1, \ldots, E_m$ be all the prime power degree cyclic subextensions of M containing K.



Then $\bigcap_{i=1}^{m} E_i = K$. Further, each extension of degree $p_i^{a_i}$ can be broken down into extensions of prime degree.

East Carolina UNIVERSITY

Extensions of degree 2 are enough

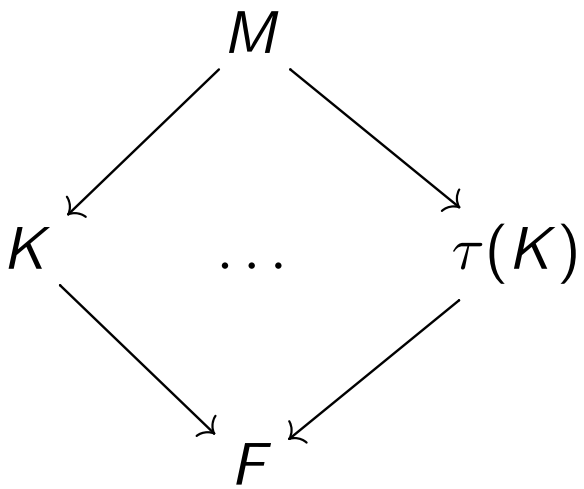
Proposition (Diophantine Stability for Extensions of Degree 2.)

If for any pair of number fields M and K such that $[M : K] = 2$ we have that the ring of integers of K is Diophantine over the ring of integers of M, then $\mathbb{Z}$ is existentially definable over the ring of integers of any number field and therefore HTP is unsolvable over the ring of integers of any number field.

East Carolina UNIVERSITY

Descent to a totally really field

Let $M/\mathbb{Q}$ be a finite Galois extension such that M is not totally real field. Let Let $K \subset \mathbb{R}$ be the fixed field of complex conjugation. Then $\bigcap_{\tau \in \mathrm{Gal}(M/\mathbb{Q})} \tau(K)$ is a totally real subfield of M. Further, for all $\tau \in \mathrm{Gal}(M/\mathbb{Q})$ it is the case $[M : \tau(K)] = 2$.



Here we let τ range over all elements of $\mathrm{Gal}(M/\mathbb{Q})$.

East Carolina University

Outline

East Carolina University

Can we use abelian varieties, not just elliptic curves?

One expects the same types of theorems as for elliptic curves. In other words if we have an extension M/K of number fields and an abelian variety A defined over K such that $\text{rank}(A(K)) = \text{rank}(A(M))$ then O_K is Diophantine over O_M. (Work in progress, S. and B. Mazur)

Finitely generated abelian varieties over infinite extensions of $\mathbb{Q}$ can also be used to show existential and first-order undecidability of these fields.

East Carolina UNIVERSITY

New results of Mazur and Rubin on Diophantine stability

Definition

Suppose V is an irreducible algebraic variety over K. If L is a field containing K, we say that V is Diophantine-stable for L/K if $V(L) = V(K)$. If ℓ is a rational prime, we say that V is ℓ-Diophantine-stable over K if for every positive integer n, and every finite set $\mathcal{S}$ of places of K, there are infinitely many cyclic extensions L/K of degree ℓ^n, totally split at all places $v \in \mathcal{S}$, such that $V(L) = V(K)$.

Theorem

Suppose A is a simple abelian variety over K and all $\bar{K}$ -endomorphisms of A are defined over K. Then there is a set $\mathcal{S}$ of rational primes with positive density such that A is ℓ-Diophantine-stable over K for every $\ell \in \mathcal{S}$.

East Carolina UNIVERSITY