The World of Definability In Number Theory

according to Alexandra Shlapentokh

East Carolina University,
Greenville, North Carolina, USA

September 30, 2016
The World of Definability In Number Theory

Prologue

Outline

1 Prologue
   - Some Questions and Answers
2 Becoming More Ambitious
3 Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News
4 Big and Small
5 Poonen’s Model
6 What if?
7 Going up
8 Into infinity
   - Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of $\mathbb{Q}$
   - Generalizing Definability Results of Videla and Fukuzaki
   - New Undecidability Results
   - Using Finitely Generated Elliptic Curves
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
Who Proved the First-Order Theory of $\mathbb{Z}$ is Undecidable?

- “Grundlagen der Mathematik”, by David Hilbert and Paul Bernays, 1934-39, Springer
The World of Definability in Number Theory

Prologue

Some Questions and Answers

Number Field Results of Julia Robinson

---

**Theorem (1949)**

\[ \mathbb{Z} \text{ is definable by a first-order formula over } \mathbb{Q}. \text{ Thus the first-order theory of } \mathbb{Q} \text{ (in the language of rings) is undecidable.} \]

---

**Theorem (1959)**

If \( K \) is a number field, then \( \mathbb{Z} \) is definable over \( O_K \) (the ring of integers of \( K \)) by a first-order formula (using just one universal quantifier and several existential quantifiers). Thus the first-order theory of \( O_K \) (in the language of rings) is undecidable.

---

**Remark**

That particular definition of the ring of algebraic integers \( O_K \) given by Julia Robinson depended on the number field \( K \). It used explicitly the degree of the field and monic irreducible polynomials of the basis elements. Later on she constructed a uniform definition not depending on a particular number field.
The World of Definability in Number Theory

Prologue

Some Questions and Answers

Number Field Results of Julia Robinson

**Theorem (1949)**

\[ \mathbb{Z} \text{ is definable by a first-order formula over } \mathbb{Q}. \text{ Thus the first-order theory of } \mathbb{Q} \text{ (in the language of rings) is undecidable.} \]

**Theorem (1959)**

If \( K \) is a number field, then \( \mathbb{Z} \) is definable over \( O_K \) (the ring of integers of \( K \)) by a first-order formula (using just one universal quantifier and several existential quantifiers). Thus the first-order theory of \( O_K \) (in the language of rings) is undecidable.

**Remark**

That particular definition of the ring of algebraic integers \( O_K \) given by Julia Robinson depended on the number field \( K \). It used explicitly the degree of the field and monic irreducible polynomials of the basis elements. Later on she constructed a uniform definition not depending on a particular number field.
The World of Definability In Number Theory
Prologue
Some Questions and Answers

Number Field Results of Julia Robinson

**Theorem (1949)**

\[ \mathbb{Z} \text{ is definable by a first-order formula over } \mathbb{Q}. \text{ Thus the first-order theory of } \mathbb{Q} \text{ (in the language of rings) is undecidable.} \]

**Theorem (1959)**

*If* \( K \) *is a number field, then* \( \mathbb{Z} \) *is definable over* \( O_K \) *(the ring of integers of* \( K \)) *by a first-order formula (using just one universal quantifier and several existential quantifiers). Thus the first-order theory of* \( O_K \) *(in the language of rings) is undecidable.*

**Remark**

That particular definition of the ring of algebraic integers \( O_K \) given by Julia Robinson depended on the number field \( K \). It used explicitly the degree of the field and monic irreducible polynomials of the basis elements. Later on she constructed a uniform definition not depending on a particular number field.
The 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. In other words it was shown that $HTP(\mathbb{Z})$, considered as a set of indices of polynomials with roots in $\mathbb{Z}$, is Turing equivalent to the Halting Set.
Recursive, Recursively Enumerable Sets.

**Definition (Recursive Sets)**
A subset of integers is called *recursive or computable* if there is an algorithm to determine membership in the set.

**Definition (Recursively Enumerable Sets)**
A subset of integers is called *recursively (or computably) enumerable* if there is an algorithm to list the elements of the set.

**Theorem**
*There are r.e. sets that are not recursive.*
Recursive, Recursively Enumerable Sets.

**Definition (Recursive Sets)**

A subset of integers is called *recursive or computable* if there is an algorithm to determine membership in the set.

**Definition (Recursively Enumerable Sets)**

A subset of integers is called *recursively (or computably) enumerable* if there is an algorithm to list the elements of the set.

**Theorem**

*There are r.e. sets that are not recursive.*
The World of Definability In Number Theory
Prologue
Some Questions and Answers

Recursive, Recursively Enumerable Sets.

**Definition (Recursive Sets)**
A subset of integers is called *recursive or computable* if there is an algorithm to determine membership in the set.

**Definition (Recursively Enumerable Sets)**
A subset of integers is called *recursively (or computably) enumerable* if there is an algorithm to list the elements of the set.

**Theorem**
*There are r.e. sets that are not recursive.*
Let \( \phi_n \) be the \( n \)-th program or algorithm. Let

\[
K = \{ n \in \mathbb{Z}_{>0} | \phi_n(n) \text{ converges or terminates} \}.
\]

Then \( K \) is called the **Halting Set**.
Turing Reducibility

Deciding membership using an oracle

Given $A, B \subseteq \mathbb{Z}$ we say that $A$ is Turing reducible to $B$ ($A \leq_T B$) if we can effectively determine membership of $A$ from the characteristic function of $B$.

Theorem

Every r.e. set is Turing reducible to the Halting Set.
Turing Reducibility

Deciding membership using an oracle

Given $A, B \subseteq \mathbb{Z}$ we say that $A$ is Turing reducible to $B$ ($A \leq_T B$) if we can effectively determine membership of $A$ from the characteristic function of $B$.

Theorem

*Every r.e. set is Turing reducible to the Halting Set.*
Diophantine Sets: a Number-Theoretic Definition

For an integral domain $R$, a subset $A \subseteq R^m$ 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

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

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

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.
Diophantine Sets: a Number-Theoretic Definition

For an integral domain $R$, a subset $A \subseteq R^m$ 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

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

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

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.
The World of Definability In Number Theory
Prologue
Some Questions and Answers

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.
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.
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.
Another Corollary of MDRP

**Corollary**

Consider an effective listing all polynomials over \( \mathbb{Z} \) and let \( \text{HTP}(\mathbb{Z}) \) be the set of indices of polynomials with solutions in \( \mathbb{Z} \). Then \( \text{HTP}(\mathbb{Z}) \equiv_T K \).

**Proof.**

Since \( \text{HTP}(\mathbb{Z}) \) is r.e., we have \( \text{HTP}(\mathbb{Z}) \leq_T K \), and since \( K \) is Diophantine, we have \( K \leq_T \text{HTP}(\mathbb{Z}) \).
Corollary

Consider an effective listing all polynomials over \( \mathbb{Z} \) and let \( HTP(\mathbb{Z}) \) be the set of indices of polynomials with solutions in \( \mathbb{Z} \). Then \( HTP(\mathbb{Z}) \equiv_T K \).

Proof.

Since \( HTP(\mathbb{Z}) \) is r.e., we have \( HTP(\mathbb{Z}) \leq_T K \), and since \( K \) is Diophantine, we have \( K \leq_T HTP(\mathbb{Z}) \).
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).
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).
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).
Outline

1 Prologue
   - Some Questions and Answers

2 Becoming More Ambitious

3 Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News

4 Big and Small

5 Poonen’s Model

6 What if?

7 Going up

8 Into infinity
   - Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of $\mathbb{Q}$
   - Generalizing Definability Results of Videla and Fukuzaki
   - New Undecidability Results Using Finitely Generated Elliptic Curves
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.
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.
Undecidability of HTP over $\mathbb{Q}$ Implies
Undecidability of HTP for $\mathbb{Z}$

Indeed, suppose we knew how to determine whether solutions exist over $\mathbb{Z}$. Let $Q(x_1, \ldots, x_k)$ be a polynomial with rational coefficients. Then

$$\exists x_1, \ldots, x_k \in \mathbb{Q} : Q(x_1, \ldots, x_k) = 0$$

$$
\uparrow
$$

$$\exists y_1, \ldots, y_k, z_1, \ldots, z_k \in \mathbb{Z} : Q\left(\frac{y_1}{z_1}, \ldots, \frac{y_k}{z_k}\right) = 0 \land z_1 \ldots z_k \neq 0.$$

So decidability of HTP over $\mathbb{Z}$ would imply the decidability of HTP over $\mathbb{Q}$. 
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 \( p(T, \vec{X}) \) 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.

\[
\begin{align*}
  h(T_1, \ldots, T_l) &= 0 \\
  p(T_1, \vec{X}_1) &= 0 \\
  &
\end{align*}
\]

...\[
\begin{align*}
  &
  p(T_l, \vec{X}_l) = 0
\end{align*}
\]

(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 \( \mathbb{Z} \).
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.

\[
\begin{align*}
    h(T_1, \ldots, T_l) &= 0 \\
p(T_1, \bar{X}_1) &= 0 \\
    \cdots \\
p(T_l, \bar{X}_l) &= 0
\end{align*}
\]

(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 $\mathbb{Z}$.
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 World of Definability In Number Theory

Complications

Outline

1 Prologue
   - Some Questions and Answers

2 Becoming More Ambitious

3 Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News

4 Big and Small

5 Poonen’s Model

6 What if?

7 Going up

8 Into infinity
   - Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of $\mathbb{Q}$
   - Generalizing Definability Results of Videla and Fukuzaki
   - New Undecidability Results
   - Using Finitely Generated Elliptic Curves
A Conjecture of Barry Mazur

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.

A Nasty Consequence

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

Remark

If the conjecture is true, no infinite and discrete (in the archimedean topology) set has a Diophantine definition over $\mathbb{Q}$. 
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.

A Nasty Consequence

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

Remark

If the conjecture is true, no infinite and discrete (in the archimedean topology) set has a Diophantine definition over $\mathbb{Q}$. 
A Conjecture of Barry Mazur

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.

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

Remark
If the conjecture is true, no infinite and discrete (in the archimedean topology) set has a Diophantine definition over $\mathbb{Q}$. 
What is a Diophantine Model of $\mathbb{Z}$?

Let $R$ be a recursive ring whose fraction field is not algebraically closed and let $\phi : \mathbb{Z} \rightarrow R^k$ be a recursive injection mapping Diophantine sets of $\mathbb{Z}$ to Diophantine sets of $R^k$. Then $\phi$ is called a Diophantine model of $\mathbb{Z}$ over $R$. 
Diophantine Model of $\mathbb{Z}$ Implies Undecidability

If $R$ has a Diophantine model of $\mathbb{Z}$, then $R$ has undecidable Diophantine sets. Indeed, let $A \subset \mathbb{Z}$ be an undecidable Diophantine set. Suppose we want to determine whether an integer $n \in A$. Instead of answering this question directly we can ask whether $\phi(n) \in \phi(A)$. By assumption $\phi(n)$ is algorithmically computable. So if $\phi(A)$ is a computable subset of $R$, we have a contradiction.
Diophantine Model of $\mathbb{Z}$ Implies Undecidability

If $R$ has a Diophantine model of $\mathbb{Z}$, then $R$ has undecidable Diophantine sets. Indeed, let $A \subset \mathbb{Z}$ be an undecidable Diophantine set. Suppose we want to determine whether an integer $n \in A$. Instead of answering this question directly we can ask whether $\phi(n) \in \phi(A)$. By assumption $\phi(n)$ is algorithmically computable. So if $\phi(A)$ is a computable subset of $R$, we have a contradiction.

HTP($R$) $\equiv_T$ Halting Set

One can also show that if $R$ has a Diophantine model of $\mathbb{Z}$, then HTP($R$) is also Turing equivalent to the Halting Set.
The World of Definability In Number Theory

Complications

Introducing New Models

Another Breakthrough Idea

So all we need is a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$!!!!
The World of Definability in Number Theory

Complications

More Bad News

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 \( \mathbb{Q} \).
If Mazur’s conjecture on topology of rational points holds, then there is no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$. 
The World of Definability In Number Theory
Big and Small

The rings between the ring of integers and a number field

A Ring in between
Let $S$ be a set of primes of a number field $K$. Let $O_{K,S}$ be the following subring of $K$.

$$\{ x \in K \mid \text{ord}_p x \geq 0, \forall p \notin S \}$$

If $S = \emptyset$, then $O_{K,S} = O_K$ – the ring of integers of $K$. If $S$ contains all the primes of $K$, then $O_{K,S} = K$. If $S$ is finite, we call the ring small (or the ring of $S$-integers). If $S$ is infinite, we call the ring big, and if the natural density of $S$ is equal to 1, we call the ring very big.
Definability World: First Glance

\[ \mathbb{Q} \overset{\text{finite}}{\longrightarrow} O_{\mathbb{Q},\nu} \longrightarrow \ldots \longrightarrow O_{\mathbb{Q},\omega} \longrightarrow \ldots \longrightarrow O_{\mathbb{Q},s} \overset{\text{finite}}{\longrightarrow} \mathbb{Z} \]
Defining Integers over Small Subrings of Number Fields

**Theorem (Julia Robinson)**

$O_K$ has a Diophantine definition over any small subring of any number field $K$, including $\mathbb{Q}$.

**Corollary**

HTP is unsolvable over all small subrings of $\mathbb{Q}$ and is Turing equivalent to the Halting Set.
Defining Integers over Small Subrings of Number Fields

Theorem (Julia Robinson)

$O_K$ has a Diophantine definition over any small subring of any number field $K$, including $\mathbb{Q}$.

Corollary

$HTP$ is unsolvable over all small subrings of $\mathbb{Q}$ and is Turing equivalent to the Halting Set.
Outline

1 Prologue
   - Some Questions and Answers
2 Becoming More Ambitious
3 Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News
4 Big and Small
5 Poonen’s Model
6 What if?
7 Going up
8 Into infinity
   - Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of $\mathbb{Q}$
   - Generalizing Definability Results of Videla and Fukuzaki
   - New Undecidability Results Using Finitely Generated Elliptic Curves
Existential Model of \( \mathbb{Z} \) over a Very Big Subring

**Theorem**

There exist recursive sets of primes \( T_1 \) and \( T_2 \), both of natural density zero and with an empty intersection, such that for any set \( S \) of primes containing \( T_1 \) and avoiding \( T_2 \), the following hold:

- \( \mathbb{Z} \) has a Diophantine model over \( O_{\mathbb{Q},S} \).
- Hilbert’s Tenth Problem is undecidable over \( O_{\mathbb{Q},S} \).

(Poonen, 2003)
Complementary Subrings

**Theorem**

For every $t > 1$ and every collection $\delta_1, \ldots, \delta_t$ of nonnegative computable real numbers (i.e. real numbers which can be approximated by a sequence of computable numbers) adding up to 1, the set of primes of $\mathbb{Q}$ may be partitioned into $t$ mutually disjoint recursive subsets $S_1, \ldots, S_t$ of natural densities $\delta_1, \ldots, \delta_t$, respectively, with the property that each ring $O_{\mathbb{Q},S_i}$ has a Diophantine model of $\mathbb{Z}$ and thus has an undecidable HTP Turing equivalent to the Halting Set. (Eisentraeger, Everest 09, Perlega 11, Eisenträger, Everest, S. 11)
The World of Definability In Number Theory

What if?

Outline

1 Prologue
   - Some Questions and Answers
2 Becoming More Ambitious
3 Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News
4 Big and Small
5 Poonen’s Model
6 What if?
7 Going up
8 Into infinity
   - Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of \( \mathbb{Q} \)
   - Generalizing Definability Results of Videla and Fukuzaki
   - New Undecidability Results
      Using Finitely Generated Elliptic Curves
So far, as one can see, all the attempts to resolve the Diophantine status of $\mathbb{Q}$ and the big rings were centered around attempts to prove (sometimes successfully) that these rings (including $\mathbb{Q}$) were like $\mathbb{Z}$ as far as the Turing class of their Diophantine problem is concerned. The natural (at least for a computability theorist) question which arises here is whether $\text{HTP}(\mathbb{Q}) \equiv_T \text{HTP}(\mathbb{Z})$ in the case $\text{HTP}(\mathbb{Q})$ is undecidable. In other words, *the Diophantine problem of $\mathbb{Q}$ may be undecidable and yet “easier” than the Diophantine problem of $\mathbb{Z}$*, and this would account for the lack of success in attempts to produce the Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ or an algorithm for solving polynomial equations over $\mathbb{Q}$.
So far, as one can see, all the attempts to resolve the Diophantine status of \( \mathbb{Q} \) and the big rings were centered around attempts to prove (sometimes successfully) that these rings (including \( \mathbb{Q} \)) were like \( \mathbb{Z} \) as far as the Turing class of their Diophantine problem is concerned. The natural (at least for a computability theorist) question which arises here is whether \( \text{HTP}(\mathbb{Q}) \equiv_T \text{HTP}(\mathbb{Z}) \) in the case \( \text{HTP}(\mathbb{Q}) \) is undecidable. In other words, the Diophantine problem of \( \mathbb{Q} \) may be undecidable and yet “easier” than the Diophantine problem of \( \mathbb{Z} \), and this would account for the lack of success in attempts to produce the Diophantine model of \( \mathbb{Z} \) over \( \mathbb{Q} \) or an algorithm for solving polynomial equations over \( \mathbb{Q} \).
What we knew for a long time

Proposition (Julia Robinson)

Let $S$ contain all but finitely many primes. Then $\text{HTP}(O_{\mathbb{Q},S}) \leq_T \text{HTP}(\mathbb{Q})$.

Proposition

Let $R$ be any big or small ring. Then $\text{HTP}(\mathbb{Q}) \leq_T \text{HTP}(R)$.
What we knew for a long time

Proposition (Julia Robinson)
Let $S$ contain all but finitely many primes. Then
$$\text{HTP}(O_{\mathbb{Q},S}) \leq_{T} \text{HTP}(\mathbb{Q}).$$

Proposition
Let $R$ be any big or small ring. Then $\text{HTP}(\mathbb{Q}) \leq_{T} \text{HTP}(R).$
New Results For C. E. Sets

Theorem (Eisenträger, Miller, Park, S.)
There exists a sequence \( \mathcal{P} = \mathcal{W}_0 \supseteq \mathcal{W}_1 \supseteq \mathcal{W}_2 \ldots \) of c.e. sets of rational primes (with \( \mathcal{P} \) denoting the set of all primes) such that

1. \( HTP(O_{\mathbb{Q}, \mathcal{W}_i}) \equiv_T HTP(\mathbb{Q}) \) for \( i \in \mathbb{Z}_{>0} \),
2. \( \mathcal{W}_{i-1} \setminus \mathcal{W}_i \) has the relative upper density (with respect to \( \mathcal{W}_{i-1} \)) equal to 1 for all \( i \in \mathbb{Z}_{>0} \),
3. The lower density of \( \mathcal{W}_i \) is 0, for \( i \in \mathbb{Z}_{>0} \).

Theorem (Eisenträger, Miller, Park, S.)
For any computable real number \( r \) between 0 and 1 there exists a c.e. set \( \mathcal{S} \) of primes such that the lower density \( \mathcal{S} \) is \( r \) and \( HTP(O_{\mathbb{Q}, \mathcal{S}}) \equiv_T HTP(\mathbb{Q}) \).
The World of Definability In Number Theory
What if?

New Results For C. E. Sets

**Theorem (Eisenträger, Miller, Park, S.)**

There exists a sequence $\mathcal{P} = \mathcal{W}_0 \supset \mathcal{W}_1 \supset \mathcal{W}_2 \ldots$ of c.e. sets of rational primes (with $\mathcal{P}$ denoting the set of all primes) such that

1. $HTP(O_{\mathbb{Q}, \mathcal{W}_i}) \equiv_T HTP(\mathbb{Q})$ for $i \in \mathbb{Z}_{>0}$,
2. $\mathcal{W}_{i-1} \setminus \mathcal{W}_i$ has the relative upper density (with respect to $\mathcal{W}_{i-1}$) equal to 1 for all $i \in \mathbb{Z}_{>0}$,
3. The lower density of $\mathcal{W}_i$ is 0, for $i \in \mathbb{Z}_{>0}$.

**Theorem (Eisenträger, Miller, Park, S.)**

For any computable real number $r$ between 0 and 1 there exists a c.e. set $S$ of primes such that the lower density $S$ is $r$ and $HTP(O_{\mathbb{Q}, S}) \equiv_T HTP(\mathbb{Q})$. 
The World of Definability In Number Theory
What if?

Definability World: Second Glance

\[ \mathbb{Q} \quad O_{\mathbb{Q}, \mathbb{V}} \quad \ldots \quad O_{\mathbb{Q}, \mathbb{W}} \quad \ldots \quad O_{\mathbb{Q}, \mathbb{W}'} \quad \ldots \quad O_{\mathbb{Q}, \mathbb{S}} \quad \mathbb{Z} \]

\[ \leq_T \quad \text{definability} \quad \text{definability} \quad \text{definability} \quad \leq_T \]
Some Questions Without an Answer and a Remarkable Theorem

Let $\mathcal{W}_1$ be an infinite and co-infinite set of rational primes, let $p \notin \mathcal{W}_1$ and let $\mathcal{W}_2 = \mathcal{W}_1 \cup \{p\}$.

- Is $O_{\mathbb{Q},\mathcal{W}_2} = \mathbb{Z}[\mathcal{W}_2^{-1}]$ existentially definable (as a set of pairs) over $O_{\mathbb{Q},\mathcal{W}_1} = \mathbb{Z}[\mathcal{W}_1^{-1}]$?
- Is $\text{HTP}(\mathbb{Z}[\mathcal{W}_2^{-1}]) \leq_T \text{HTP}(\mathbb{Z}[\mathcal{W}_1^{-1}])$?
- Can we define $\mathbb{Z}$ existentially in any big ring?

**Theorem (Koenigsmann 16)**

There exists a definition of $\mathbb{Z}$ over $\mathbb{Q}$ of the form

$$\forall \exists \ldots \exists f(...)=0,$$

where $f$ is a polynomial, with only one variable in the scope of the universal quantifier.
Let $\mathcal{W}_1$ be an infinite and co-infinite set of rational primes, let $p \notin \mathcal{W}_1$ and let $\mathcal{W}_2 = \mathcal{W}_1 \cup \{p\}$.

- Is $O_{\mathbb{Q},\mathcal{W}_2} = \mathbb{Z}[\mathcal{W}_2^{-1}]$ existentially definable (as a set of pairs) over $O_{\mathbb{Q},\mathcal{W}_1} = \mathbb{Z}[\mathcal{W}_1^{-1}]$?
- Is $HTP(\mathbb{Z}[\mathcal{W}_2^{-1}]) \leq_T HTP(\mathbb{Z}[\mathcal{W}_1^{-1}])$?
- Can we define $\mathbb{Z}$ existentially in any big ring?

**Theorem (Koenigsmann 16)**

*There exists a definition of $\mathbb{Z}$ over $\mathbb{Q}$ of the form $\forall \exists \ldots \exists f(\ldots) = 0$, where $f$ is a polynomial, with only one variable in the scope of the universal quantifier.*
Outline

1. Prologue
   - Some Questions and Answers
2. Becoming More Ambitious
3. Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News
4. Big and Small
5. Poonen’s Model
6. What if?
7. Going up
8. Into infinity
   - Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of $\mathbb{Q}$
   - Generalizing Definability Results of Videla and Fukuzaki
   - New Undecidability Results Using Finitely Generated Elliptic Curves
The World of Definability In Number Theory
Going up

The Rings of Integers of Number Fields

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)
It would suffice

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 $\text{rank } E(M) = \text{rank } E(K) > 0$, 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)
It would suffice

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 $\text{rank } E(M) = \text{rank } E(K) > 0$, then $\mathbb{Z}$ is existentially definable over the ring of integers of any number field and therefore $\text{HTP}$ 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)
If $K$ is a totally real number field, an extension of degree 2 of a totally real number field or such that there exists an elliptic curve defined over $\mathbb{Q}$ and of the same positive rank over $K$ and $\mathbb{Q}$, then for any $\varepsilon > 0$, there exists a set $W$ of primes of $K$ whose natural density is bigger than $1 - [K : \mathbb{Q}]^{-1} - \varepsilon$ and such that $\mathbb{Z}$ has a diophantine definition over $O_{K,W}$, thus implying that Hilbert’s Tenth Problem is undecidable over $O_{K,W}$. (S. 97, 00, 02, 08)

Assume there is an elliptic curve defined over $K$ with $K$-rank equal to 1. For every $t > 1$ and every collection $\delta_1, \ldots, \delta_t$ of nonnegative computable real numbers adding up to 1, the set of primes of $K$ may be partitioned into $t$ mutually disjoint computable subsets $S_1, \ldots, S_t$ of natural densities $\delta_1, \ldots, \delta_t$, respectively, with the property that $\mathbb{Z}$ admits a diophantine model in each ring $O_{K,S_i}$. In particular, Hilbert’s Tenth Problem is undecidable for each ring $O_{K,S_i}$. (Poonen, S 05, Eisentraeger, Everest 09, Perlega 11, Eisentraeger, Everest, S. 11)
The World of Definability In Number Theory
Going up

Big Subrings of Number Fields from the Point of View of $\mathbb{Q}$

**Theorem (Eisentraeger, Miller, Park, S. 16)**

There exists a sequence $\mathcal{P} = \mathcal{W}_0 \supset \mathcal{W}_1 \supset \mathcal{W}_2 \ldots$ of c.e. sets of primes of a number field $K$ (with $\mathcal{P}$ denoting the set of all primes of $K$) such that

1. $\text{HTP}(O_K, \mathcal{W}_i) \equiv_T \text{HTP}(K) \leq_T \text{HTP}(\mathbb{Q})$ for $i \in \mathbb{Z}_{>0}$,
2. $\mathcal{W}_{i-1} - \mathcal{W}_i$ has the relative upper density (with respect to $\mathcal{W}_{i-1}$) equal to 1 for all $i \in \mathbb{Z}_{>0}$,
3. The lower density of $\mathcal{W}_i$ is 0, for all $i \in \mathbb{Z}_{>0}$.

**Corollary**

There exists a computably enumerable subset $\mathcal{W}$ of $K$-primes, of lower natural density 0, such that

$\text{HTP}(\mathbb{Q}) \geq_T \text{HTP}(K) \equiv_T \text{HTP}(O_K, \mathcal{W})$. 
The World of Definability In Number Theory

Definability World: Third Glance

\[ \mathbb{Q} \rightarrow O_{\mathbb{Q},\mathcal{V}} \rightarrow O_{\mathbb{Q},\mathcal{W}} \rightarrow O_{K,\mathcal{W}_K} \rightarrow \cdots \]

\[ \leq_T \]

\[ K \leftarrow O_{K,\mathcal{V}_K} \rightarrow O_{K,\mathcal{W}_K} \rightarrow \cdots \]

\[ \leq_T \]

\[ \mathbb{Z} \leftarrow O_{\mathbb{Q},\mathcal{W}} \rightarrow O_{\mathbb{Q},\mathcal{W}} \rightarrow \cdots \]

\[ \leq_T \]

\[ O_{K,\mathcal{W}_K} \rightarrow \cdots \rightarrow O_{K,\mathcal{S}} \rightarrow O_K \]

\[ \leq_T \]

\[ O_{K,\mathcal{S}} \rightarrow O_K \rightarrow \cdots \]

\[ \leq_T \]
The World of Definability In Number Theory

Outline

1. Prologue
   - Some Questions and Answers
2. Becoming More Ambitious
3. Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News
4. Big and Small
5. Poonen’s Model
6. What if?
7. Going up
8. Into infinity
   - Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of $\mathbb{Q}$
   - Generalizing Definability Results of Videla and Fukuzaki
   - New Undecidability Results Using Finitely Generated Elliptic Curves
What are we seeking out there?

For the purposes of our discussion we fix an algebraic closure \( \bar{\mathbb{Q}} \) of \( \mathbb{Q} \) and consider a progression from \( \mathbb{Q} \) to its algebraic closure, first through the finite extensions of \( \mathbb{Q} \), next through its infinite extensions fairly “far” from the algebraic closure, and finally through the infinite extensions of \( \mathbb{Q} \) fairly “close” to \( \bar{\mathbb{Q}} \).

As one gets closer to \( \bar{\mathbb{Q}} \), there is an expectation that the language of rings would loose more and more of its expressive power. It would be interesting to describe the mile posts signifying various stages of this loss.
Two Questions

Question

If $K_{\text{inf}}$ is an infinite algebraic extension of $\mathbb{Q}$, then is the ring of integers of $K_{\text{inf}}$ first-order definable over $K_{\text{inf}}$?

Question

Is the first-order theory of $K_{\text{inf}}$ decidable?
Two Questions

**Question**

If $K_{\text{inf}}$ is an infinite algebraic extension of $\mathbb{Q}$, then is the ring of integers of $K_{\text{inf}}$ first-order definable over $K_{\text{inf}}$?

**Question**

Is the first-order theory of $K_{\text{inf}}$ decidable?
The World of Definability In Number Theory
Into infinity
Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of $\mathbb{Q}$

Results of Rumeley and van den Dries for the Ring of All Algebraic Integers

Theorem (R. Rumely, 1986)

*Hilbert’s Tenth Problem is decidable over the ring of all algebraic integers.*

Theorem (L. van den Dries, 1988)

*First-order theory of the ring of all algebraic integers is decidable.*
Results of Rumeley and van den Dries for the
Ring of All Algebraic Integers

**Theorem (R. Rumely, 1986)**

*Hilbert’s Tenth Problem is decidable over the ring of all algebraic integers.*

**Theorem (L. van den Dries, 1988)**

*First-order theory of the ring of all algebraic integers is decidable.*
The first-order theory of the field of all totally real algebraic numbers is decidable.
Results of Julia Robinson for Totally Real Infinite Extensions of $\mathbb{Q}$

**Theorem (1962)**

*If a family $\mathcal{F}$ of sets of a totally real algebraic integer ring $R$ containing arbitrarily large finite sets can be arithmetically defined in $R$, then the natural numbers can be defined arithmetically in $R$. Hence $R$ is undecidable.*

**Corollary (1962)**

*The natural numbers can be defined arithmetically in any totally real algebraic integer ring $R$ such that there is a smallest interval $(0, s)$, $s$ real or $\infty$, which contains infinitely many sets of conjugates of numbers of $R$, i.e., infinitely many $x \in R$ with all the conjugates (over $\mathbb{Q}$) in $(0, s)$.***
Results of Julia Robinson for Totally Real Infinite Extensions of \( \mathbb{Q} \)

**Theorem (1962)**

If a family \( \mathcal{F} \) of sets of a totally real algebraic integer ring \( R \) containing arbitrarily large finite sets can be arithmetically defined in \( R \), then the natural numbers can be defined arithmetically in \( R \). Hence \( R \) is undecidable.

**Corollary (1962)**

The natural numbers can be defined arithmetically in any totally real algebraic integer ring \( R \) such that there is a smallest interval \( (0, s) \), \( s \) real or \( \infty \), which contains infinitely many sets of conjugates of numbers of \( R \), i.e., infinitely many \( x \in R \) with all the conjugates (over \( \mathbb{Q} \)) in \( (0, s) \).
Proposition (Kronecker, 1857)

The interval $(0, 4)$ contains infinitely many sets of conjugates of totally real algebraic integers and no sub-interval of $(0, 4)$ does.

Corollary

The ring of algebraic integers of any totally real field containing an infinite set of the form \{\(\cos \frac{2\pi}{k} j, k_j \in J\)\} has an undecidable first-order theory. In particular, the first-order theory of the ring of all totally real integers is undecidable.

Proof.

\[2 \cos \frac{2\pi}{k} = \xi_k + \xi_k^{-1},\] where \(\xi_k\) is a \(k\)-th primitive root of unity. So \(2 \cos \frac{2\pi}{k}\) is an algebraic integers with all conjugates over \(\mathbb{Q}\) of the form \(2 \cos \frac{2\pi r}{k}\) for some \(r\) relatively prime to \(k\). Hence \(4 \cos^2 \left( \frac{2\pi}{k} \right)\) is a totally positive integer in the interval \((0, 4)\).
Undecidability Results for Totally Real Rings

**Proposition (Kronecker, 1857)**

The interval $(0, 4)$ contains infinitely many sets of conjugates of totally real algebraic integers and no sub-interval of $(0, 4)$ does.

**Corollary**

The ring of algebraic integers of any totally real field containing an infinite set of the form \( \{\cos \frac{2\pi}{kj}, kj \in J\} \) has an undecidable first-order theory. In particular, the first-order theory of the ring of all totally real integers is undecidable.

**Proof.**

\[ 2 \cos \frac{2\pi}{k} = \xi_k + \xi_k^{-1}, \] where \( \xi_k \) is a \( k \)-th primitive root of unity. So \( 2 \cos \frac{2\pi}{k} \) is an algebraic integers with all conjugates over \( \mathbb{Q} \) of the form \( 2 \cos \frac{2\pi r}{k} \) for some \( r \) relatively prime to \( k \). Hence \( 4 \cos^2 \left( \frac{2\pi}{k} \right) \) is a totally positive integer in the interval \((0, 4)\).
Undecidability Results for Totally Real Rings

**Proposition (Kronecker, 1857)**

The interval $(0, 4)$ contains infinitely many sets of conjugates of totally real algebraic integers and no sub-interval of $(0, 4)$ does.

**Corollary**

The ring of algebraic integers of any totally real field containing an infinite set of the form $\{\cos 2\pi/k_j, k_j \in J\}$ has an undecidable first-order theory. In particular, the first-order theory of the ring of all totally real integers is undecidable.

**Proof.**

$2 \cos 2\pi/k = \xi_k + \xi_k^{-1}$, where $\xi_k$ is a $k$-th primitive root of unity. So $2 \cos 2\pi/k$ is an algebraic integers with all conjugates over $\mathbb{Q}$ of the form $2 \cos 2\pi r/k$ for some $r$ relatively prime to $k$. Hence $4 \cos^2(2\pi/k)$ is a totally positive integer in the interval $(0, 4)$. □
The World of Definability In Number Theory
Into infinity
Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of \( \mathbb{Q} \)

Another undecidability result by Julia Robinson

**Theorem (1962)**

The first-order theory of the ring of integers of \( \mathbb{Q}(\sqrt{b}, b \in B) \), \( B \) – an infinite set of positive integers, is undecidable.

Julia Robinson showed that in this case \( s \) is infinite.
Videla’s Results on pro-$p$ Extensions


If $K_{inf}$ is an infinite extension of a number field $K$, such that the degrees of all finite subextensions are divisible by a fixed (for the field) finite set of primes, then the ring of integers of $K_{inf}$ is first-order definable over $K_{inf}$.

**Corollary**

The first-order theory of $\mathbb{Q}(\sqrt{b}, b \in B)$, $B$ – an infinite set of positive integers, is undecidable.
Videla’s Results on pro-$p$ Extensions


If $K_{inf}$ is an infinite extension of a number field $K$, such that the degrees of all finite subextensions are divisible by a fixed (for the field) finite set of primes, then the ring of integers of $K_{inf}$ is first-order definable over $K_{inf}$.

**Corollary**

The first-order theory of $\mathbb{Q}(\sqrt{b}, b \in B)$, $B$ – an infinite set of positive integers, is undecidable.
The first-order theory of the ring of integers $\mathbb{Q}(\xi_p^k, k \in \mathbb{Z}_{>0})$ is undecidable.

Corollary

The first-order theory of $\mathbb{Q}(\xi_p^k, k \in \mathbb{Z}_{>0})$ is undecidable.

Remark

The proof also showed that for some finite sets of primes $\mathcal{P}$ the results hold over $\mathbb{Q}(\xi_p^k, k \in \mathbb{Z}_{>0}), p \in \mathcal{P}$
The World of Definability in Number Theory
Into infinity
Some History of First-Order Definability and Decidability over Infinite Algebraic Extensions of \( \mathbb{Q} \)

**Videla’s Results on Cyclotomastics**


The first-order theory of the ring of integers \( \mathbb{Q}(\xi_{p^k}, k \in \mathbb{Z}_{>0}) \) is undecidable.

**Corollary**

The first-order theory of \( \mathbb{Q}(\xi_{p^k}, k \in \mathbb{Z}_{>0}) \) is undecidable.

**Remark**

The proof also showed that for some finite sets of primes \( \mathcal{P} \) the results hold over \( \mathbb{Q}(\xi_{p^k}, k \in \mathbb{Z}_{>0}), p \in \mathcal{P} \)
The first-order theory of the ring of integers $\mathbb{Q}(\xi_{p^k}, k \in \mathbb{Z}_{>0})$ is undecidable.

Corollary

The first-order theory of $\mathbb{Q}(\xi_{p^k}, k \in \mathbb{Z}_{>0})$ is undecidable.

Remark

The proof also showed that for some finite sets of primes $\mathcal{P}$ the results hold over $\mathbb{Q}(\xi_{p^k}, k \in \mathbb{Z}_{>0}), p \in \mathcal{P}$
Fukuzaki’s Results

**Theorem (2012)**

A ring of integers is definable over an infinite Galois extension of the rationals and its subextensions if every finite subextension of the Galois extension has odd degree over the rationals and its prime ideals dividing 2 are unramified.

**Corollary (2012)**

The first order theory of \( \mathbb{Q}(\cos(2\pi/l^n) : l \in \mathcal{P}, n \in \mathbb{Z}_{>0}) \), with \( \mathcal{P} \) is a set of primes equivalent to -1 mod 4, is undecidable.
Fukuzaki’s Results

**Theorem (2012)**

A ring of integers is definable over an infinite Galois extension of the rationals and its subextensions if every finite subextension of the Galois extension has odd degree over the rationals and its prime ideals dividing 2 are unramified.

**Corollary (2012)**

The first order theory of $\mathbb{Q}(\cos(2\pi/\ell^n) : \ell \in \mathcal{P}, n \in \mathbb{Z}_{>0})$, with $\mathcal{P}$ is a set of primes equivalent to -1 mod 4, is undecidable.
Let $K_{\text{inf}}$ be an algebraic (possibly infinite) extension of a number field $K$ and let $q$ be a rational prime number. Let $p_K$ be a prime of $K$.

- Suppose there exists a positive integer $n$ such that for any number field $M$ with $K \subset M \subset K_{\text{inf}}$ for at least one prime $p_M$ of $M$ we have that $\text{ord}_q[M_{p_M} : K_{p_K}] \leq n$. In this case we say that $p_K$ is $q$-bounded.

- If for every number field $M$ with $K \subset M \subset K_{\text{inf}}$ and every $p_M$ above $p_K$, we also have that $p_M$ is $q$-bounded, then we say that $p_K$ is hereditarily $q$-bounded.

- Finally, if for all $M$ and all $p_M$ we have $\text{ord}_q[M_{p_M} : K_{p_K}] \leq n$, then we say that $p_K$ is completely $q$-bounded.

If every prime of $K$ is hereditarily $q$-bounded and factors of $q$ are completely $q$-bounded, then we call $K_{\text{inf}}$ a $q$-bounded field.
The Main Definability Result

**Theorem**

If $q$ is any rational prime and $K_{inf}$ is an algebraic $q$-bounded extension of $\mathbb{Q}$, then the ring of integers of $K_{inf}$ is first-order definable over $K_{inf}$. 
Finite Extensions of $q$-bounded Fields

Proposition

A finite extension of a $q$-bounded field is $q$-bounded.
Examples of $q$-bounded Galois Extensions

**Example**

If $K_{\inf}$ is a Galois extension of a number field $K$ such that for any number field $M \subset K_{\inf}$, we have that $[M : K] \not\equiv 0 \mod q$, then $O_{K_{\inf}}$, the ring of integers of $K_{\inf}$, is first-order definable over $K_{\inf}$. This example covers cyclotomic extensions with finitely many ramified primes, i.e. extensions of the form $\mathbb{Q}(\xi_{p_1^\ell}, \ldots, \xi_{p_k^\ell}, \ell \in \mathbb{Z}_{>0})$, where $p_1, \ldots, p_k$ are rational primes, and all their subfields that include all abelian extensions with finitely many ramified primes.

**Example**

Given a prime $q$, and an integer $m > 0$, our method also applies to the case of a cyclotomic extension generated by any set $\{\xi_{p^\ell}, \ell \in \mathbb{Z}_{>0}\}$ and all its subfields, as long as long as $p \neq q$ and $q^{m+1} \nmid (p - 1)$. 
Examples of $q$-bounded Galois Extensions

Example

If $K_{\text{inf}}$ is a Galois extension of a number field $K$ such that for any number field $M \subset K_{\text{inf}}$, we have that $[M : K] \not\equiv 0 \mod q$, then $O_{K_{\text{inf}}}$, the ring of integers of $K_{\text{inf}}$, is first-order definable over $K_{\text{inf}}$. This example covers cyclotomic extensions with finitely many ramified primes, i.e. extensions of the form $\mathbb{Q}(\xi_{p_1^\ell}, \ldots, \xi_{p_k^\ell}, \ell \in \mathbb{Z}_{>0})$, where $p_1, \ldots, p_k$ are rational primes, and all their subfields that include all abelian extensions with finitely many ramified primes.

Example

Given a prime $q$, and an integer $m > 0$, our method also applies to the case of a cyclotomic extension generated by any set $\{\xi_{p^\ell}, \ell \in \mathbb{Z}_{>0}\}$ and all its subfields, as long as long as $p \neq q$ and $q^{m+1} \not| (p - 1)$. 
Fukuzaki’s Fields Updated

Example

Given a prime $q$, and an integer $m > 0$, the first-order theory of any totally real subfield of a cyclotomic extension generated by any set $\{\xi_p^\ell, \ell \in \mathbb{Z}_{>0}\}$ is undecidable, as long as long as $p \neq q$, $q^{m+1} \nmid (p - 1)$ and the field contains infinitely many “cosines”. For example the first-order theory of the largest totally real subfield of this cyclotomic is undecidable.
**Theorem**

Any totally real $q$-bounded field has a totally real extension with undecidable first-order theory.

**Proof.**

Let $p \not\equiv 1 \mod q$ and let $K_{\inf}$ be totally real and $q$-bounded. In this case $K_{\inf}(\cos(2\pi/p^k, k \in \mathbb{Z}_{>0})$ is totally real and $q$-bounded.
Extending Videla’s Undecidability Result

**Theorem**

Let $A$ be an abelian extension of $\mathbb{Q}$ with finitely many ramified primes. In this case the first-order theory of $A$ is undecidable.
Theorem

Let $q$ be a rational prime and let $K_{inf}$ be an infinite algebraic extension of $\mathbb{Q}$ with at least one prime of a number field contained in $\mathbb{Q}$ completely $q$-bounded. Assume also there exist an elliptic curve defined over $K_{inf}$ such that its Mordell-Weil group has positive rank and is finitely generated. In this case $\mathbb{Z}$ is first-order definable over this field and therefore the first-order theory of this field is undecidable.
Why $q$-bounded?

- $q$ be a rational prime number,
- $K$ be a number field containing a primitive $q$-th root of unity,
- $p_K$ be a prime of $K$ not dividing $q$,
- $b \in K$ be such that $\text{ord}_{p_K} b = -1$,
- $c \in K$ be such that $c$ is integral at $p_K$ and is not a $q$-th power in the residue field of $p_K$,

and consider $bx^q + b^q$. Note that $\text{ord}_{p_K}(bx^q + b^q)$ is divisible by $q$ if and only if $\text{ord}_{p_K} x \geq 0$. Further, if $x$ is an integer, all the poles of $bx^q + b^q$ must be poles of $b$ and are divisible by $q$. Assume also that all zeros of $bx^q + b^q$ and all zeros and poles of $c$ are of orders divisible by $q$ and $c \equiv 1 \mod q^3$. Finally, to simplify the situation further, assume that either $K$ has no real embeddings into $\bar{\mathbb{Q}}$ or $q > 2$. 
Now consider the norm equation

\[ N_{K(\sqrt{c})/K}(y) = bx^q + b^q. \]  

(2)

Since \( p_K \) does not split in this extension, if \( x \) has a pole at \( p_K \), then \( \text{ord}_{p_K} bx^q + b^q \not\equiv 0 \mod q \), and the norm equation has no solution \( y \) in \( K(\sqrt{c}) \). Further, if \( x \) is an integer, given our assumptions, using the Hasse Norm Principle we can show that this norm equation does have a solution. Our conditions on \( c \) insure that the extension is unramified, and our conditions on \( bx^q + b^q \) in the case \( x \) is an integer make sure that locally \textit{at every prime not splitting in the extension} the element \( bx^q + b^q \) is equal to a \( q \)-th power of some element of the local field times a unit. By the Local Class Field Theory, this makes \( bx^q + b^q \) a norm locally at every prime.
For an arbitrary $b$ and $c \equiv 1 \mod q^3$ in $K$, we will not necessarily have all zeros of $bx^q + b^q$ and all zeros and poles of $c$ of orders divisible by $q$. For this reason, given $x, b, c \in K$ we consider our norm equation in a finite extension $L$ of $K$ and this extension $L$ depends on $x, b, c$ and $q$. We choose $L$ so that all primes occurring as zeros of $bx^q + b^q$ or as zeros or poles of $c$ are ramified with ramification degree divisible by $q$. We also take care to split $p_K$ completely in $L$, so that in $L$ we still have that $c$ is not a $q$-th power modulo any factor of $p_L$. This way, as we run through all $b, c \in K$ with $c - 1 \equiv 0 \mod q^3$, we “catch” all the primes that do not divide $q$ and occur as poles of $x$. 
Let $d_1, \ldots, d_n$ be rational integers $\geq 2$. The compositum $K$ of all totally real abelian extensions of $\mathbb{Q}$ of degree $d$ ranging in $d_1, \ldots, d_n$ is of infinite degree and its first order theory is undecidable.