Easy as \( \mathbb{Q} \): Hilbert’s Tenth Problems for Subrings of \( \mathbb{Q} \) and Number Fields

Alexandra Shlapentokh

East Carolina University,
Greenville, North Carolina, USA

April 17, 2014
Easy as $\mathbb{Q}$: Hilbert’s Tenth Problems for Subrings of $\mathbb{Q}$ and Number Fields

Prologue

Outline

1. **Prologue**
   - A Question and the Answer
   - Some Easy Facts
   - Becoming More Ambitious

2. **Complications**
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News

3. **Big and Small**

4. **Poonen’s Model**

5. **What if?**

6. **A Small Improvement of the Old Result**
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
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. 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.
Diophantine Sets: a Number-Theoretic Definition

A subset $A \subset \mathbb{Z}^m$ is called Diophantine over $\mathbb{Z}$ if there exists a polynomial $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ with rational integer coefficients such that for any element $(t_1, \ldots, t_m) \in \mathbb{Z}^m$ we have that

$$\exists x_1, \ldots, x_k \in \mathbb{Z}: p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\iff$$

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

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

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

A subset $A \subset \mathbb{Z}^m$ is called Diophantine over $\mathbb{Z}$ if there exists a polynomial $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ with rational integer coefficients such that for any element $(t_1, \ldots, t_m) \in \mathbb{Z}^m$ we have that

$$\exists x_1, \ldots, x_k \in \mathbb{Z}: p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$\uparrow \downarrow$

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

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

Remark

Diophantine sets can also be described as the sets existentially definable in the language of rings or as projections of algebraic sets.
Easy as $\mathbb{Q}$: Hilbert’s Tenth Problems for Subrings of $\mathbb{Q}$ and Number Fields

Prologue

Some Easy Facts

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 $A_1 \cap A_2$. 

\[\square\]
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 $A_1 \cap A_2$. 

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

Lemma (Replacing Finitely Many by One)

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.

Proof.
Consider a system of equations

\[
\begin{align*}
g_1(x_1, \ldots, x_k) &= 0 \\
g_2(x_1, \ldots, x_k) &= 0 \\
& \quad \quad \quad \vdots \\
g_m(x_1, \ldots, x_k) &= 0
\end{align*}
\]

This system has solutions in \( \mathbb{Z} \) if and only if the following equation has solutions in \( \mathbb{Z} \):

\[
g_1(x_1, \ldots, x_k)^2 + g_2(x_1, \ldots, x_k)^2 + \ldots + g_m(x_1, \ldots, x_k)^2 = 0
\]
One vs. Finitely Many

Lemma (Replacing Finitely Many by One)

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.

Proof.

Consider a system of equations

$$\begin{cases} g_1(x_1, \ldots, x_k) = 0 \\ g_2(x_1, \ldots, x_k) = 0 \\ \vdots \\ g_m(x_1, \ldots, x_k) = 0 \end{cases}$$

This system has solutions in $\mathbb{Z}$ if and only if the following equation has solutions in $\mathbb{Z}$:

$$g_1(x_1, \ldots, x_k)^2 + g_2(x_1, \ldots, x_k)^2 + \ldots + g_m(x_1, \ldots, x_k)^2 = 0$$
One vs. Finitely Many

Lemma (Replacing Finitely Many by One)

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.

Proof.

Consider a system of equations

\[
\begin{align*}
g_1(x_1, \ldots, x_k) &= 0 \\
g_2(x_1, \ldots, x_k) &= 0 \\
&\quad \ldots \\
g_m(x_1, \ldots, x_k) &= 0
\end{align*}
\]

This system has solutions in \( \mathbb{Z} \) if and only if the following equation has solutions in \( \mathbb{Z} \):

\[g_1(x_1, \ldots, x_k)^2 + g_2(x_1, \ldots, x_k)^2 + \ldots + g_m(x_1, \ldots, x_k)^2 = 0\]
Corollary

We can let the Diophantine definitions consist of several polynomials without changing the nature of the relation.
A Very Useful Diophantine Definition

**Proposition**

The set of non-zero integers has the following Diophantine definition:

\[ \{ t \in \mathbb{Z} | \exists x, u, v \in \mathbb{Z} : (2u - 1)(3v - 1) = tx \} \]

**Proof.**

If \( t = 0 \), then either \( 2u - 1 = 0 \) or \( 3v - 1 = 0 \) has a solution in \( \mathbb{Z} \), which is impossible.

Suppose now \( t \neq 0 \). Write \( t = t_2t_3 \), where \( t_2 \) is odd and \( t_3 \neq 0 \) mod 3. Then since \( (t_2, 2) = 1 \) and \( (t_3, 3) = 1 \), by a property of GCD there exist \( u, x_u, v, x_v \in \mathbb{Z} \) such that \( 2u + t_2x_u = 1 \) and \( 3v + t_3x_v = 1 \). Then \( (2u - 1)(3v - 1) = t_2x_u t_3x_v = t(x_u x_v) \). \( \Box \)
Some Easy Facts

A Very Useful Diophantine Definition

**Proposition**

The set of non-zero integers has the following Diophantine definition:

\[ \{ t \in \mathbb{Z} | \exists x, u, v \in \mathbb{Z} : (2u - 1)(3v - 1) = tx \} \]

**Proof.**

If \( t = 0 \), then either \( 2u - 1 = 0 \) or \( 3v - 1 = 0 \) has a solution in \( \mathbb{Z} \), which is impossible.

Suppose now \( t \neq 0 \). Write \( t = t_2 t_3 \), where \( t_2 \) is odd and \( t_3 \neq 0 \) mod 3. Then since \( (t_2, 2) = 1 \) and \( (t_3, 3) = 1 \), by a property of GCD there exist \( u, x_u, v, x_v \in \mathbb{Z} \) such that \( 2u + t_2 x_u = 1 \) and \( 3v + t_3 x_v = 1 \). Then \( (2u - 1)(3v - 1) = t_2 x_u t_3 x_v = t(x_u x_v) \).
A Very Useful Diophantine Definition

Proposition

The set of non-zero integers has the following Diophantine definition:

$$\{ t \in \mathbb{Z} | \exists x, u, v \in \mathbb{Z} : (2u - 1)(3v - 1) = tx \}$$

Proof.

If $t = 0$, then either $2u - 1 = 0$ or $3v - 1 = 0$ has a solution in $\mathbb{Z}$, which is impossible.

Suppose now $t \neq 0$. Write $t = t_2t_3$, where $t_2$ is odd and $t_3 \neq 0$ mod 3. Then since $(t_2, 2) = 1$ and $(t_3, 3) = 1$, by a property of GCD there exist $u, x_u, v, x_v \in \mathbb{Z}$ such that $2u + t_2x_u = 1$ and $3v + t_3x_v = 1$. Then $(2u - 1)(3v - 1) = t_2x_ut_3x_v = t(x uxv)$. \qed
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.
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 $p(T, \bar{X})$ 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.

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

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 $\mathbb{Z}$. 

\[\square\]
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.

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

(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 \( \mathbb{Q} \)!!!
Outline

1 Prologue
   ■ A Question and the Answer
   ■ Some Easy Facts
   ■ Becoming More Ambitious

2 Complications
   ■ Some Unpleasant Thoughts
   ■ Introducing New Models
   ■ More Bad News

3 Big and Small

4 Poonen’s Model

5 What if?

6 A Small Improvement of the Old Result
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 $\mathbb{Q}$. 
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 $\mathbb{Q}$. 
Easy as $\mathbb{Q}$: Hilbert’s Tenth Problems for Subrings of $\mathbb{Q}$ and Number Fields

Complications

Some Unpleasant Thoughts

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 $\mathbb{Q}$. 
In a recent paper Jochen Koenigsmann showed that a strong form of a Bombieri-Lang conjecture also implies that there is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$. 
Another Plan: Diophantine Models

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 $R$. 
More about Diophantine Models

Sending Diophantine Sets to Diophantine Sets Makes the Map Recursive

Actually the recursiveness of the map will follow from the fact that the $\phi$-image of the graph of addition is Diophantine. Indeed, if the $\phi$-image of the graph of addition is Diophantine, it is recursively enumerable. So we have an effective listing of the set

$$D_+ = \{(\phi(m), \phi(n), \phi(m + n)), m, n \in \mathbb{Z}\}.$$ 

Assume we have computed $\phi(k - 1)$. Now start listing $D_+$ until we come across a triple whose first two entries are $\phi(k - 1)$ and $\phi(1)$. Then the third element of the triple must be $\phi(k)$. 
More about Diophantine Models

Sending Diophantine Sets to Diophantine Sets Makes the Map Recursive

Actually the recursiveness of the map will follow from the fact that the \( \phi \)-image of the graph of addition is Diophantine. Indeed, if the \( \phi \)-image of the graph of addition is Diophantine, it is recursively enumerable. So we have an effective listing of the set

\[
D_+ = \{(\phi(m), \phi(n), \phi(m + n)), m, n \in \mathbb{Z}\}.
\]

Assume we have computed \( \phi(k - 1) \). Now start listing \( D_+ \) until we come across a triple whose first two entries are \( \phi(k - 1) \) and \( \phi(1) \). Then the third element of the triple must be \( \phi(k) \).
Sending Diophantine Sets to Diophantine Sets Makes the Map Recursive

Actually the recursiveness of the map will follow from the fact that the $\phi$-image of the graph of addition is Diophantine. Indeed, if the $\phi$-image of the graph of addition is Diophantine, it is recursively enumerable. So we have an effective listing of the set

$$D_+ = \{ (\phi(m), \phi(n), \phi(m + n)), m, n \in \mathbb{Z} \}.$$ 

Assume we have computed $\phi(k - 1)$. Now start listing $D_+$ until we come across a triple whose first two entries are $\phi(k - 1)$ and $\phi(1)$. Then the third element of the triple must be $\phi(k)$. 
Making Addition and Multiplication Diophantine is Enough

Theorem

To make a map $\phi : \mathbb{Z} \rightarrow R$ into a Diophantine model, it is enough to require that the $\phi$-images of the graphs of $\mathbb{Z}$-addition and $\mathbb{Z}$-multiplication are Diophantine over $R$. 

Proof.
Boring induction.
Making Addition and Multiplication Diophantine is Enough

**Theorem**

To make a map $\phi : \mathbb{Z} \rightarrow R$ into a Diophantine model, it is enough to require that the $\phi$-images of the graphs of $\mathbb{Z}$-addition and $\mathbb{Z}$-multiplication are Diophantine over $R$.

**Proof.**

Boring induction.
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.
Easy as $\mathbb{Q}$: Hilbert’s Tenth Problems for Subrings of $\mathbb{Q}$ and Number Fields

Complications

Introducing New Models

Another Breakthrough Idea

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 $\mathbb{Q}$. 
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 \( \mathbb{Q} \).
Outline

1. Prologue
   - A Question and the Answer
   - Some Easy Facts
   - Becoming More Ambitious

2. Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News

3. Big and Small

4. Poonen’s Model

5. What if?

6. A Small Improvement of the Old Result
A Ring in between

Let $S$ be a set of primes of $\mathbb{Q}$. Let $O_{\mathbb{Q},S}$ be the following subring of $\mathbb{Q}$.

\[
\left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, n \text{ is divisible by primes of } S \text{ only} \right\}
\]

If $S = \emptyset$, then $O_{\mathbb{Q},S} = \mathbb{Z}$. If $S$ contains all the primes of $\mathbb{Q}$, then $O_{\mathbb{Q},S} = \mathbb{Q}$. If $S$ is finite, we call the ring **small**. If $S$ is infinite, we call the ring **large**, and if the natural density of $S$ is equal to 1, we call the ring **very large**.

Definition (Natural Density)

Let $A$ be a set of primes. Then the natural density of $A$ is equal to the limit below (if it exists):

\[
\lim_{X \to \infty} \frac{\#\{p \in A, p \leq X\}}{\#\{p \leq X\}}
\]
The Rings between \( \mathbb{Z} \) and \( \mathbb{Q} \)

**A Ring in between**

Let \( S \) be a set of primes of \( \mathbb{Q} \). Let \( \mathcal{O}_{\mathbb{Q},S} \) be the following subring of \( \mathbb{Q} \).

\[
\left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, \text{n is divisible by primes of } S \text{ only} \right\}
\]

If \( S = \emptyset \), then \( \mathcal{O}_{\mathbb{Q},S} = \mathbb{Z} \). If \( S \) contains all the primes of \( \mathbb{Q} \), then \( \mathcal{O}_{\mathbb{Q},S} = \mathbb{Q} \). If \( S \) is finite, we call the ring **small**. If \( S \) is infinite, we call the ring **large**, and if the natural density of \( S \) is equal to 1, we call the ring **very large**.

**Definition (Natural Density)**

Let \( \mathcal{A} \) be a set of primes. Then the natural density of \( \mathcal{A} \) is equal to the limit below (if it exists):

\[
\lim_{X \to \infty} \frac{\#\{p \in \mathcal{A}, p \leq X\}}{\#\{p \leq X\}}
\]
Example of a Small Ring not Equal to $\mathbb{Z}$

$$\left\{ \frac{m}{3^a5^b} : m \in \mathbb{Z}, a, b \in \mathbb{Z}_{>0} \right\}$$

Example of a Big Ring not Equal to $\mathbb{Q}$

$$\left\{ \frac{m}{\prod p_i^{n_i}} : p_i \equiv 1 \mod 4, n_i \in \mathbb{Z}_{>0} \right\}$$

Remark

Observe that $\mathbb{Q}$ is the fraction field of any small or big ring.
Example of a Small Ring not Equal to $\mathbb{Z}$

$$\left\{ \frac{m}{3^a5^b} : m \in \mathbb{Z}, a, b \in \mathbb{Z}_{>0} \right\}$$

Example of a Big Ring not Equal to $\mathbb{Q}$

$$\left\{ \frac{m}{\prod p_i^{n_i}} : p_i \equiv 1 \mod 4, n_i \in \mathbb{Z}_{>0} \right\}$$

Remark

Observe that $\mathbb{Q}$ is the fraction field of any small or big ring.
Example of a Small Ring not Equal to $\mathbb{Z}$

$$\left\{ \frac{m}{3^a 5^b} : m \in \mathbb{Z}, a, b \in \mathbb{Z}_{>0} \right\}$$

Example of a Big Ring not Equal to $\mathbb{Q}$

$$\left\{ \frac{m}{\prod p_i^{n_i}} : p_i \equiv 1 \mod 4, n_i \in \mathbb{Z}_{>0} \right\}$$

Remark

Observe that $\mathbb{Q}$ is the fraction field of any small or big ring.
Proposition

1. The set of non-zero elements of a big or a small ring is Diophantine over the ring.

2. “One=finitely many” over big and small rings.
Diophantine Properties of Big and Small Rings

Proposition

1. The set of non-zero elements of a big or a small ring is Diophantine over the ring.
2. “One=finitely many” over big and small rings.
Defining Integers over Small Subrings of \( \mathbb{Q} \)

**Theorem (Julia Robinson)**

\( \mathbb{Z} \) has a Diophantine definition over any small subring of \( \mathbb{Q} \).

**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 $\mathbb{Q}$

**Theorem (Julia Robinson)**

$\mathbb{Z}$ has a Diophantine definition over any small subring of $\mathbb{Q}$.

**Corollary**

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

1 Prologue
   - A Question and the Answer
   - Some Easy Facts
   - Becoming More Ambitious

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

3 Big and Small

4 Poonen’s Model

5 What if?

6 A Small Improvement of the Old Result
Existential Model of $\mathbb{Z}$ over a Very Large 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 (Eisenträger, Everest, S. 2011)

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 $\mathcal{O}_{\mathbb{Q}, S_i}$ has a Diophantine model of $\mathbb{Z}$ and thus has an undecidable HTP Turing equivalent to the Halting Set.
Outline

1. Prologue
   - A Question and the Answer
   - Some Easy Facts
   - Becoming More Ambitious

2. Complications
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News

3. Big and Small

4. Poonen’s Model

5. What if?

6. A Small Improvement of the Old Result
So far

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

\[ HTP(O_{\mathbb{Q},S}) \leq_T HTP(\mathbb{Q}). \]

**Proposition**

Let $R$ be any big or small ring. Then

\[ HTP(\mathbb{Q}) \leq_T HTP(R). \]
What we knew for a long time

**Proposition (Julia Robinson)**

Let $S$ contain all but finitely many primes. Then

$$HTP(O_{\mathbb{Q},S}) \leq_T HTP(\mathbb{Q}).$$

**Proposition**

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

Theorem (Eisenträger, Miller, Park, S.: work in progress)

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. $\text{HTP}(O_{\mathbb{Q},\mathcal{W}_i}) \equiv_T \text{HTP}(\mathbb{Q})$ 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.: work in progress)

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 $\text{HTP}(O_{\mathbb{Q},S}) \equiv_T \text{HTP}(\mathbb{Q})$. 

New Results For C. E. Sets

Theorem (Eisenträger, Miller, Park, S.: work in progress)
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.: work in progress)
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 \( HTP(O_{\mathbb{Q}, S}) \equiv_T HTP(\mathbb{Q}) \).
Examples where HTP is no more complicated than the ring itself

Theorem (Eisenträger, Miller, Park, S.: work in progress)

For every computably enumerable set $B \subset \mathbb{Z}_{>0}$ with $HTP(\mathbb{Q}) \leq_T B$, there exists a ring $R = O_{\mathbb{Q},S}$, with $S$ a computably enumerable subset of the prime numbers of lower density 0, such that $S \equiv_T R \equiv_T HTP(R) \equiv_T B$. (By setting $B \equiv_T HTP(\mathbb{Q})$, we can thus make $HTP(R) \equiv_T HTP(\mathbb{Q})$, of course.)
Results for Sets Computable in $\text{HTP}(\mathbb{Q})$

**Theorem (Eisenträger, Miller, Park, S.: work in progress)**

For any positive integer $m$, the set of all rational primes $\mathcal{P}$ can be represented as a union of pairwise disjoint sets $S_0, \ldots, S_{m-1}$, each of upper density 1 and such that for all $i$ we have that $\text{HTP}(O_{\mathbb{Q},S_i}) \leq T \text{HTP}(\mathbb{Q})$ and $S_i \leq T \text{HTP}(\mathbb{Q})$.

**Theorem (Eisenträger, Miller, Park, S.: work in progress)**

There exist infinitely many subsets $S_0, S_1, \ldots$ of the set $\mathcal{P}$ of primes, all of lower density 0, all computable uniformly from an $\text{HTP}(\mathbb{Q})$-oracle (so that the rings $R_j = O_{\mathbb{Q},S_j}$ are also uniformly computable below $\text{HTP}(\mathbb{Q})$), which have $\bigcup_j S_j = \mathcal{P}$ and $S_i \cap S_j = \emptyset$ for all $i < j$, and such that $\text{HTP}(O_{\mathbb{Q},S_j}) \equiv_T \text{HTP}(\mathbb{Q})$ for every $j$. 
Results for Sets Computable in $\text{HTP}(\mathbb{Q})$

**Theorem (Eisenträger, Miller, Park, S.: work in progress)**

For any positive integer $m$, the set of all rational primes $\mathcal{P}$ can be represented as a union of pairwise disjoint sets $S_0, \ldots, S_{m-1}$, each of upper density 1 and such that for all $i$ we have that $\text{HTP}(\mathbb{O}_\mathbb{Q}, S_i) \leq_T \text{HTP}(\mathbb{Q})$ and $S_i \leq_T \text{HTP}(\mathbb{Q})$.

**Theorem (Eisenträger, Miller, Park, S.: work in progress)**

There exist infinitely many subsets $S_0, S_1, \ldots$ of the set $\mathcal{P}$ of primes, all of lower density 0, all computable uniformly from an $\text{HTP}(\mathbb{Q})$-oracle (so that the rings $R_j = \mathbb{O}_\mathbb{Q}, S_j$ are also uniformly computable below $\text{HTP}(\mathbb{Q})$), which have $\bigcup_j S_j = \mathcal{P}$ and $S_i \cap S_j = \emptyset$ for all $i < j$, and such that $\text{HTP}(\mathbb{O}_\mathbb{Q}, S_j) \equiv_T \text{HTP}(\mathbb{Q})$ for every $j$. 
Easy as $\mathbb{Q}$: Hilbert’s Tenth Problems for Subrings of $\mathbb{Q}$ and Number Fields

A Small Improvement of the Old Result

Outline

1. **Prologue**
   - A Question and the Answer
   - Some Easy Facts
   - Becoming More Ambitious

2. **Complications**
   - Some Unpleasant Thoughts
   - Introducing New Models
   - More Bad News

3. **Big and Small**

4. **Poonen’s Model**

5. **What if?**

6. **A Small Improvement of the Old Result**
Theorem

For every finite set \( S \) of primes, \( \text{HTP}(O_{\mathbb{Q},S}) \) is computable uniformly in \( \text{HTP}(\mathbb{Q}) \). That is, there exists an algorithm which accepts as input any finite set of primes \( p_1, \ldots, p_n \) and outputs the code number \( e \) for a program using \( \text{HTP}(\mathbb{Q}) \) as an oracle such that \( \Phi_e^{\text{HTP}(\mathbb{Q})} \) computes the characteristic function of \( \text{HTP}(O_{\mathbb{Q},\{p_1,\ldots,p_n\}}) \).
A Simple Construction, I

Notation
- Let $\{f_e\}_{e \in \mathbb{Z}_{>0}} \in \mathbb{Z}[X_1, X_2, \ldots]$ be an effective enumeration of polynomials.
- Let $S_n$ denote the primes inverted by the end of Stage $n$.
- Let $\overline{S}_n$ be a list of primes which have been put on a "do not invert" list by the end of Stage $n$.
- Let $S_0 = \emptyset$, and $\overline{S}_0 = \emptyset$. 
A Simple Construction, II

Assume we have just completed Stage $n$. Now consider the polynomial equation $f_{n+1}(\bar{X}) = 0$ and use the $\text{HTP}(\mathbb{Q})$-oracle to determine whether this polynomial equation has solutions in the semilocal ring where the primes of $\mathcal{S}_n$ are not inverted. If the answer is "no", then $f_{n+1}$ is put on the list of polynomials without solutions in our ring. If the answer is "yes", then we add the polynomial to the list of polynomials with solutions in our ring and search for a solution integral at primes in $\mathcal{S}_n$. Once we locate the solution, we add all the primes which appear in the denominators of this solution to $\mathcal{S}_n$ to form $\mathcal{S}_{n+1}$. Finally we add an arbitrary finite set of not yet processed primes to $\mathcal{S}_n$ to form $\mathcal{S}_{n+1}$. We let $S = \bigcup_{n=0}^{\infty} S_n$ and conclude that $S \leq_T \text{HTP}(\mathbb{Q})$ and $\text{HTP}(\mathcal{O}_{\mathbb{Q}, S}) \leq_T \text{HTP}(\mathbb{Q})$. 
We let
\[ E := \{ (f, \vec{x}, j) : f \in \mathbb{Z}[X_1, \ldots, X_n], \vec{x} \in \mathbb{Q}^n, n \in \mathbb{Z}, j \in \mathbb{Z}_{>0} \} \]
and
we let \( g : \mathbb{Z}_{>0} \to E \) be a bijection.

For each \( e > 0 \), we introduce a boolean variable \( R_e \). At the beginning of the construction, \( R_e \) is set to FALSE for all \( e > 0 \).

At each step \( s \), we will define the sets \( S_s \) and \( V_s \); at the end of the construction, we will define \( S = \bigcup_s S_s \).
Using Priority Argument, II

- At stage $s = 0$: let $S_0 = \emptyset$, $\mathcal{V}_0 = \emptyset$.
- At stage $s > 0$: suppose $g(s) = (f_e, \vec{x}, j) \in E$. Let

$$\mathcal{V}_s = \text{the set of the } e \text{ smallest elements not in } S_{s-1}.$$ 

Now there are two cases:

1. If $R_e = \text{FALSE}$, $\vec{x} \in O_{Q, \mathcal{V}_s}$ and $f_e(\vec{x}) = 0$, then let $S_s = S_{s-1} \cup T_s$, where $T_s$ is the least set of primes such that $\vec{x} \in (O_{Q, T_s})^n$. Here, we set $R_e = \text{TRUE}$.

2. Otherwise, $S_{s-1} = S_s$.

- In the end, let $S = \bigcup_{s=1}^{\infty} S_s$, and $R = O_{Q, S}$.

Since this construction is entirely effective, $S$ is computably enumerable, and so $R$ is computably presentable. Further, $\text{HTP}(R) \equiv_T \text{HTP}(Q)$. 