Hilbert’s Tenth Problem: Undecidability of Polynomial Equations

Alexandra Shlapentokh

East Carolina University,
Greenville, North Carolina, USA

July 2010
Table of Contents

1 Easy or Difficult?
2 Questions: Old and New
   - An Old Question
   - Diophantine Sets and Definitions
   - New Questions
3 Mazur’s Conjectures
   - The Statements of the Conjectures
   - Diophantine Models
   - A Steep Curve
   - What Now?
4 Changing the Object: Rings Big and Small
5 Definability over Small Rings
6 Definability over Big Rings
   - Poonen’s Theorem
   - The Old Plan
   - Putting Two Rings Together
7 Back to the Universal Quantifier
8 And Now for the Big Conjecture
   - Number Fields
   - What We Know Now
   - What We Might Know in the Future
Outline

1. Easy or Difficult?
2. Questions: Old and New
   - An Old Question
   - Diophantine Sets and Definitions
   - New Questions
3. Mazur’s Conjectures
   - The Statements of the Conjectures
   - Diophantine Models
   - A Steep Curve
   - What Now?
4. Changing the Object: Rings Big and Small
5. Definability over Small Rings
6. Definability over Big Rings
   - Poonen’s Theorem
   - The Old Plan
   - Putting Two Rings Together
7. Back to the Universal Quantifier
8. And Now for the Big Conjecture
   - Number Fields
   - What We Know Now
   - What We Might Know in the Future
Hilbert’s Tenth Problem: Undecidability of Polynomial Equations
Easy or Difficult?

Does this equation have integer solutions?

\[ x + y + z = 1000 \]

\[ x^4 + y^4 + z^4 = 1000000 \]

\[ x^2 + y^3 + z^4 + w^7 = 1000000 \]

\[ x_1^2 + x_2^3 + x_3^3 + x_4^4 + x_5^5 = 123001 \]
Does this equation have integer solutions?

\[ x + y + z = 1000 \]

\[ x^4 + y^4 + z^4 = 1000000 \]

\[ x^2 + y^3 + z^4 + w^7 = 1000000 \]

\[ x_1^2 + x_2^3 + x_3^3 + x_4^4 + x_5^5 = 123001 \]
Does this equation have integer solutions?

\[ x + y + z = 1000 \]

\[ x^4 + y^4 + z^4 = 1000000 \]

\[ x^2 + y^3 + z^4 + w^7 = 1000000 \]

\[ x_1^2 + x_2^3 + x_3^3 + x_4^4 + x_5^5 = 123001 \]
Hilbert’s Tenth Problem: Undecidability of Polynomial Equations
Easy or Difficult?

Does this equation have integer solutions?

\[ x + y + z = 1000 \]

\[ x^4 + y^4 + z^4 = 1000000 \]

\[ x^2 + y^3 + z^4 + w^7 = 1000000 \]

\[ x_1^2 + x_2^3 + x_3^3 + x_4^4 + x_5^5 = 123001 \]
Outline

1 Easy or Difficult?
2 Questions: Old and New
   - An Old Question
   - Diophantine Sets and Definitions
   - New Questions
3 Mazur’s Conjectures
   - The Statements of the Conjectures
   - Diophantine Models
   - A Steep Curve
   - What Now?
4 Changing the Object: Rings Big and Small
5 Definability over Small Rings
6 Definability over Big Rings
   - Poonen’s Theorem
   - The Old Plan
   - Putting Two Rings Together
7 Back to the Universal Quantifier
8 And Now for the Big Conjecture
   - Number Fields
   - What We Know Now
   - What We Might Know in the Future
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.
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.
Hilbert’s Tenth Problem: Undecidability of Polynomial Equations

Questions: Old and New

An Old Question

Hilbert’s Question about Polynomial Equations

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

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

This problem became known as Hilbert’s Tenth Problem.
The Answer

This question was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri 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 subsets of $\mathbb{Z}$.
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 subsets of $\mathbb{Z}$. 
Hilbert’s Tenth Problem: Undecidability of Polynomial Equations
Questions: Old and New

An Old Question

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

**Recursive Sets**

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

**Recursively Enumerable Sets**

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

**Theorem**

There exist recursively enumerable sets which are not recursive.
Recursive and Recursively Enumerable Subsets of $\mathbb{Z}$

**Recursive Sets**

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

**Recursively Enumerable Sets**

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

**Theorem**

There exist recursively enumerable sets which are not recursive.
Recursive and Recursively Enumerable Subsets of $\mathbb{Z}$

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

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

**Theorem**
*There exist recursively enumerable sets which are not recursive.*
Diophantine Sets

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 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 $\mathbb{Z}$.

Corollary

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

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

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

\[
\uparrow
\]

\[
(t_1, \ldots, t_m) \in A.
\]

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

Corollary

There are undecidable Diophantine subsets of \( \mathbb{Z} \).
Suppose $A \subset \mathbb{Z}$ is an undecidable Diophantine set with a Diophantine definition $P(T, X_1, \ldots, X_k)$. Assume also that we have an algorithm to determine existence of integer solutions for polynomials. Now, let $a \in \mathbb{Z}_{>0}$ and observe that $a \in A$ iff the polynomial $P(a, X_1, \ldots, X_K) = 0$ has solutions in $\mathbb{Z}^k$. So if we can answer Hilbert’s question effectively, we can determine the membership in $A$ effectively.
Diophantine Sets Are Recursively Enumerable

It is not hard to see that Diophantine sets are recursively enumerable. Given a polynomial $p(T, \bar{X})$ we can effectively list all $t \in \mathbb{Z}$ such that $p(t, \bar{X}) = 0$ has a solution $\bar{x} \in \mathbb{Z}^k$ in the following fashion. Using a recursive listing of $\mathbb{Z}^{k+1}$, we can plug each $(k+1)$-tuple into $p(T, \bar{X})$ to see if the value is 0. Each time we get a zero we add the first element of the $(k+1)$-tuple to the $t$-list.
A Simple Example of a Diophantine Set over $\mathbb{Z}$

The set of even integers

$$\{ t \in \mathbb{Z} \mid \exists w \in \mathbb{Z} : t = 2w \}$$

To construct more complicated examples we need to establish some properties of Diophantine sets.
A Simple Example of a Diophantine Set over $\mathbb{Z}$

The set of even integers

$$\{ t \in \mathbb{Z} | \exists w \in \mathbb{Z} : t = 2w \}$$

To construct more complicated examples we need to establish some properties of Diophantine sets.
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 $A_1 \cap A_2$. 

□
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.
One vs. Finitely Many

Proof.

Consider a system of equations

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

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

$$
g_1(x_1, \ldots, x_k)^2 + g_2(x_1, \ldots, x_k)^2 + \ldots + g_m(x_1, \ldots, x_k)^2 = 0
$$
Proof.

Consider a system of equations

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

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

\[
g_1(x_1, \ldots, x_k)^2 + g_2(x_1, \ldots, x_k)^2 + \cdots + g_m(x_1, \ldots, x_k)^2 = 0
\]
If $R$ is any recursive integral domain whose fraction field is not algebraically closed, then by a similar argument any finite system of polynomial equations over $R$ can be effectively replaced by a single polynomial equation over $R$ with the same $R$-solution set.

Corollary

We can let the Diophantine definitions consist of several polynomials without changing the nature of the relation.
Remarks:

If $R$ is any recursive integral domain whose fraction field is not algebraically closed, then by a similar argument any finite system of polynomial equations over $R$ can be effectively replaced by a single polynomial equation over $R$ with the same $R$-solution set.

Corollary:

We can let the Diophantine definitions consist of several polynomials without changing the nature of the relation.
Proposition

Let $a, b \in \mathbb{Z} \neq 0$ with $(a, b) = 1$. The there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. 
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 next that \( t \neq 0 \) and write \( t = t_2 t_3 \), where \( t_2 \) is odd and \( t_3 \neq 0 \mod 3 \). Now, since \( (t_2, 2) = 1 \) and \( (t_3, 3) = 1 \), by the property of GCD discussed above, 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

\[ (2u - 1)(3v - 1) = t_2x_u t_3x_v = t(x_u x_v). \]
Proposition

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

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

Proof.

If \( t = 0 \), then either \( 2u - 1 = 0 \) or \( 3v - 1 = 0 \) has a solution in \( \mathbb{Z} \), which is impossible. Suppose next that \( t \neq 0 \) and write \( t = t_2 t_3 \), where \( t_2 \) is odd and \( t_3 \equiv 0 \mod 3 \). Now, since \( (t_2, 2) = 1 \) and \( (t_3, 3) = 1 \), by the property of GCD discussed above, 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 \( (2u - 1)(3v - 1) = t_2 x_u t_3 x_v = t(x_u x_v) \).
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 next that \( t \neq 0 \) and write \( t = t_2t_3 \), where \( t_2 \) is odd and \( t_3 \not\equiv 0 \mod 3 \). Now, since \( (t_2, 2) = 1 \) and \( (t_3, 3) = 1 \), by the property of GCD discussed above, 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 \( (2u - 1)(3v - 1) = t_2x_u t_3x_v = t(x_u x_v) \). \( \square \)
The set of non-negative integers

From Lagrange’s Theorem we get the following representation of non-negative integers:

\[ \{ t \in \mathbb{Z} | \exists x_1, x_2, x_3, x_4 : t = x_1^2 + x_2^2 + x_3^2 + x_4^2 \} \]
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 and consider the following equivalent statements.

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

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

So decidability of HTP over $\mathbb{Z}$ would imply the decidability of HTP over $\mathbb{Q}$. 
Hilbert’s Tenth Problem: Undecidability of Polynomial Equations

Questions: Old and New

New Questions

Using Diophantine Definitions to Solve the Problem

**Lemma**

If $R$ is a recursive ring containing $\mathbb{Z}$ and $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over $R$ while the fraction field of $R$ is not algebraically closed, 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.

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

(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 $\mathbb{Z}$. 
Using Diophantine Definitions to Solve the Problem

**Lemma**

If $R$ is a recursive ring containing $\mathbb{Z}$ and $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over $R$ while the fraction field of $R$ is not algebraically closed, 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.

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

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 $\mathbb{Q}$!!!
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 Easy or Difficult?
2 Questions: Old and New
   - An Old Question
   - Diophantine Sets and Definitions
   - New Questions
3 Mazur’s Conjectures
   - The Statements of the Conjectures
   - Diophantine Models
   - A Steep Curve
   - What Now?
4 Changing the Object: Rings Big and Small
5 Definability over Small Rings
6 Definability over Big Rings
   - Poonen’s Theorem
   - The Old Plan
   - Putting Two Rings Together
7 Back to the Universal Quantifier
8 And Now for the Big Conjecture
   - Number Fields
   - What We Know Now
   - What We Might Know in the Future
A Conjecture of Barry Mazur

The Conjecture on the Topology of Rational Points

If $V$ is 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 $\mathbb{Q}$.

Actually if the conjecture is true, no infinite and discrete set has a Diophantine definition over $\mathbb{Q}$. 
Hilbert’s Tenth Problem: Undecidability of Polynomial Equations

Mazur’s Conjectures

The Statements of the Conjectures

A Conjecture of Barry Mazur

The Conjecture on the Topology of Rational Points

If $V$ is 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 $\mathbb{Q}$.

Actually if the conjecture is true, no infinite and discrete set has a Diophantine definition over $\mathbb{Q}$.
Mazur’s Conjectures

The Statements of the Conjectures

A Conjecture of Barry Mazur

The Conjecture on the Topology of Rational Points

If $V$ is 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 $\mathbb{Q}$.

Actually if the conjecture is true, no infinite and discrete set has a Diophantine definition over $\mathbb{Q}$. 
Suppose you are given a system of polynomial equations:

\[
\begin{align*}
P_1(x_1, \ldots, x_k) &= 0 \\
P_2(x_1, \ldots, x_k) &= 0 \\
\vdots \\
P_m(x_1, \ldots, x_k) &= 0
\end{align*}
\]

(2)

Think of solutions to this system as points in \( \mathbb{R}^k \) but consider only the points whose coordinates are rational numbers. In other words we are interested in the set

\[
RP = \{(x_1, \ldots, x_k) \in \mathbb{Q}^k : (x_1, \ldots, x_k) \text{ is a solution to system (2)}\}.
\]

Now take the topological closure of \( RP \) in \( \mathbb{R}^k \) (i.e. the points plus the “boundary”). Mazur’s conjecture asserts that the resulting set will have finitely many “connected pieces”.
Understanding Mazur’s Conjecture

Suppose you are given a system of polynomial equations:

\[
\begin{align*}
P_1(x_1, \ldots, x_k) &= 0 \\
P_2(x_1, \ldots, x_k) &= 0 \\
&\quad \vdots \\
P_m(x_1, \ldots, x_k) &= 0
\end{align*}
\]

Think of solutions to this system as points in $\mathbb{R}^k$ but consider only the points whose coordinates are rational numbers. In other words we are interested in the set

\[RP = \{(x_1, \ldots, x_k) \in \mathbb{Q}^k : (x_1, \ldots, x_k) \text{ is a solution to system (2)}\}.
\]

Now take the topological closure of $RP$ in $\mathbb{R}^k$ (i.e. the points plus the “boundary”). Mazur’s conjecture asserts that the resulting set will have finitely many “connected pieces”.

Hilbert's Tenth Problem: Undecidability of Polynomial Equations
Mazur's Conjectures
The Statements of the Conjectures

Understanding Mazur’s Conjecture

Suppose you are given a system of polynomial equations:

\[
\begin{align*}
P_1(x_1, \ldots, x_k) &= 0 \\
P_2(x_1, \ldots, x_k) &= 0 \\
&\vdots \\
P_m(x_1, \ldots, x_k) &= 0
\end{align*}
\]

Think of solutions to this system as points in $\mathbb{R}^k$ but consider only the points whose coordinates are rational numbers. In other words we are interested in the set

\[RP = \{(x_1, \ldots, x_k) \in \mathbb{Q}^k : (x_1, \ldots, x_k) \text{ is a solution to system (2)}\}.
\]

Now take the topological closure of $RP$ in $\mathbb{R}^k$ (i.e. the points plus the “boundary”). Mazur’s conjecture asserts that the resulting set will have finitely many “connected pieces”.
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 \( R \).
Another Plan: 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 $\phi(1)$. The third element of the triple must be $\phi(k)$. 
Another Plan: 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 $\phi(1)$. The third element of the triple must be $\phi(k)$. 
Another Plan: 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 $\phi(1)$. The third element of the triple must be $\phi(k)$. 
Making Addition and Multiplication Diophantine is Enough

It is enough to require that the $\phi$-images of the graphs of $\mathbb{Z}$-addition and $\mathbb{Z}$-multiplication are Diophantine over $R$. The proof proceeds by a straightforward induction argument on the number of operations in a Diophantine definition.
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.

### So all we need is a Diophantine model of \( \mathbb{Z} \) over \( \mathbb{Q} \)!!!
An old plan for building a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ involved using elliptic curves.
An old plan for building a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ involved using elliptic curves.

**What’s an elliptic curve?**

Consider an equation of the form:

$$y^2 = x^3 + ax + b,$$  \hspace{1cm} (3)

where $a, b \in \mathbb{Q}$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$. This equation defines an elliptic curve (a non-singular plane curve of genus 1).

*Figure:* This is copied from Wikipedia.
Using Elliptic Curves

An old plan for building a Diophantine model of \( \mathbb{Z} \) over \( \mathbb{Q} \) involved using elliptic curves.

What’s an elliptic curve?

Consider an equation of the form:

\[
y^2 = x^3 + ax + b,
\]

where \( a, b \in \mathbb{Q} \) and \( \Delta = -16(4a^3 + 27b^2) \neq 0 \). This equation defines an elliptic curve (a non-singular plane curve of genus 1).

Figure: This is copied from Wikipedia

All the points \( (x, y) \in \mathbb{Q}^2 \) satisfying (3) (if any) together with \( O \) – the “point at infinity” form an abelian group, i.e. there is a way to define addition on the points of an elliptic curve with \( O \) serving as the identity.
Using Elliptic Curves

Geometric Representation of the Group Law

1. \( P + Q + R = 0 \)
2. \( P + Q + Q = 0 \)
3. \( P + Q + 0 = 0 \)
4. \( P + P + 0 = 0 \)

**Figure:** This is also copied from Wikipedia
Using Elliptic Curves

Geometric Representation of the Group Law

Figure: This is also copied from Wikipedia

Group Law Formulas

Let \( P = (x_P, y_P) \), \( Q = (x_Q, y_Q) \), \( R = (x_R, y_R) \) be the points on an elliptic curve \( E \) with rational coordinates. If \( P +_E Q = R \) and \( P, Q, R \neq O \), then \( x_R = f(x_P, y_P, x_Q, y_Q) \), \( y_R = g(x_P, y_P, x_Q, y_Q) \), where \( f(z_1, z_2, z_3, z_4) \), \( g(z_1, z_2, z_3, z_4) \) are fixed (somewhat unpleasant looking) rational functions. Further, \( -P = (x_P, -y_P) \).
Using Elliptic Curves of Rank One

Finding the Right Curve

Let $E$ be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q}) \cong \mathbb{Z}$ as abelian groups. (In other words $E(\mathbb{Q})$ is of rank one and has no torsion points.) Let $P_1$ be a generator and consider a map sending an integer $n \neq 0$ to $[n]P = (x_n, y_n)$. The group law assures us that under this map the graph of addition is Diophantine. Unfortunately, it is not clear what happens to the graph of multiplication.
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 \( \mathbb{Q} \).
An Existential Crisis

An Important Question

What do Mathematicians do when they get stuck?
An Existential Crisis

An Important Question
What do Mathematicians do when they get stuck?

A Well-Known Answer
They change the problem.
An Existential Crisis

An Important Question
What do Mathematicians do when they get stuck?

A Well-Known Answer
They change the problem.

How?
A number-theorist will probably change the object or call a big conjecture to the rescue.
An Existential Crisis

An Important Question
What do Mathematicians do when they get stuck?

A Well-Known Answer
They change the problem.

How?
A number-theorist will probably change the object or call a big conjecture to the rescue.
A logician might change some aspects of the language.
An Existential Crisis

An Important Question
What do Mathematicians do when they get stuck?

A Well-Known Answer
They change the problem.

How?
A number-theorist will probably change the object or call a big conjecture to the rescue.
A logician might change some aspects of the language.

In due course all these things came to pass.
Outline

1 Easy or Difficult?
2 Questions: Old and New
   ■ An Old Question
   ■ Diophantine Sets and Definitions
   ■ New Questions
3 Mazur’s Conjectures
   ■ The Statements of the Conjectures
   ■ Diophantine Models
   ■ A Steep Curve
   ■ What Now?
4 Changing the Object: Rings Big and Small
5 Definability over Small Rings
6 Definability over Big Rings
   ■ Poonen’s Theorem
   ■ The Old Plan
   ■ Putting Two Rings Together
7 Back to the Universal Quantifier
8 And Now for the Big Conjecture
   ■ Number Fields
   ■ What We Know Now
   ■ What We Might Know in the Future
The Rings between $\mathbb{Z}$ and $\mathbb{Q}$

A Ring in between

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

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

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 $O_{\mathbb{Q},S} = \mathbb{Z}$. 
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 $O_{\mathbb{Q},S} = \mathbb{Q}$. 
The Rings between $\mathbb{Z}$ and $\mathbb{Q}$

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.

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 $\mathbb{Q}$

\[{\frac{m}{\prod p_i^{n_i}} : p_i \equiv 1 \mod 4, n_i \in \mathbb{Z}_{>0}}\]
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.
Lemma

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

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

Corollary

Let $R$ be a big or a small ring. Let $A \subseteq \mathbb{Q}^m$ be Diophantine over $\mathbb{Q}$. Then $A \cap R^m$ is Diophantine over $R$. 
Proposition

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

Proposition

1. “One=finitely many” over big and small rings.

2. The set of non-negative elements of a big or a small ring $R$ is Diophantine over $R$: a small modification of the Lagrange argument is required to accommodate possible denominators

$$\{ t \in R | \exists x_1, x_2, x_3, x_4, x_5 : x_5^2 t = x_1^2 + x_2^2 + x_3^2 + x_4^2 \land x_5 \neq 0 \}$$
Outline

1 Easy or Difficult?
2 Questions: Old and New
   - An Old Question
   - Diophantine Sets and Definitions
   - New Questions
3 Mazur’s Conjectures
   - The Statements of the Conjectures
   - Diophantine Models
   - A Steep Curve
   - What Now?
4 Changing the Object: Rings Big and Small
5 Definability over Small Rings
6 Definability over Big Rings
   - Poonen’s Theorem
   - The Old Plan
   - Putting Two Rings Together
7 Back to the Universal Quantifier
8 And Now for the Big Conjecture
   - Number Fields
   - What We Know Now
   - What We Might Know in the Future
Defining Integers over Small Subrings of $\mathbb{Q}$

**Theorem (Julia Robinson)**

$\mathbb{Z}$ has a Diophantine definition over any small subring of $\mathbb{Q}$ and therefore HTP is undecidable over any small ring.
Outline

1 Easy or Difficult?
2 Questions: Old and New
   - An Old Question
   - Diophantine Sets and Definitions
   - New Questions
3 Mazur’s Conjectures
   - The Statements of the Conjectures
   - Diophantine Models
   - A Steep Curve
   - What Now?
4 Changing the Object: Rings Big and Small
5 Definability over Small Rings
6 Definability over Big Rings
   - Poonen’s Theorem
   - The Old Plan
   - Putting Two Rings Together
7 Back to the Universal Quantifier
8 And Now for the Big Conjecture
   - Number Fields
   - What We Know Now
   - What We Might Know in the Future
The Statement of Poonen’s Theorem

Theorem (2003)

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 $O_{\mathbb{Q},S}$. 
What is Natural Density?

Definition

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

$$\lim_{X \to \infty} \frac{\#\{p \in A, p \leq X\}}{\#\{p \leq X\}}$$
We start with an elliptic curve of rank one. As in the past it has an equation of the form

\[ y^2 = x^3 + ax + b \]

with \( 4a^3 + 27b^2 \neq 0 \). We can choose \( a, b \in \mathbb{Z} \) and a set of primes \( S \) so that in \( O_{\mathbb{Q},S} \) all the solutions \((x, y)\) to this equation with \( y > 0 \) constitute the set

\[ \{(x_i, y_i)\} \cup \{ \text{finite set of pairs} \}, \]

where \( |y_j - j| < 10^{-j} \). Note that we know how to define positive numbers using a variation on Lagrange’s theme and how to get rid of a finite set of undesirable values (just say “\( \neq \)”).
Constructing a Model of $\mathbb{Z}_{>0}$ using $y_j$'s

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

$$D^+ = \{(y_i, y_j, y_k) \in D^3 : k = i + j, k, i, j \in \mathbb{Z}_{>0}\}$$

and

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

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

It is easy to show that

\[ k = i + j \iff |y_i + y_j - y_k| < 1/3. \]

and with the help of Lagrange this makes \( D_+ \) Diophantine. Similarly we have that

\[ k = i^2 \iff |y_i^2 - y_k| < 2/5, \]

implying that \( D_2 \) is Diophantine.
The Old Plan: Defining Multiplication of Indices

**Theorem (S. 2009)**

*Then there exists a set of primes $\mathcal{W}$ of natural density one, and an elliptic curve of rank one such that “multiplication of indices” has a Diophantine definition over $O_{\mathbb{Q}, \mathcal{W}}$.***

**What happens in this ring?**

We select a set of primes $\mathcal{W}$ so that among other things no point on our chosen elliptic curve has its coordinates in the ring. So coordinates of $(x_n, y_n)$ of $[n]P$, the $n$-th multiple of some point $P$ on our elliptic curve of infinite order, are represented by a quadruple $(U_n, V_n, A_n, B_n)$ with $x_n = \frac{U_n}{V_n}$ and $y_n = \frac{A_n}{B_n}$ with $U_n, V_n, A_n, B_n \in O_{\mathbb{Q}, \mathcal{W}}$. (A point $P$ of infinite order is a point such that $[n]P \neq 0$ for any non-zero $n$.) Unfortunately this representation is not unique. At the same time, we show that the set of 12-tuples of the form $(U_{n_1}, V_{n_1}, A_{n_1}, B_{n_1}, U_{n_2}, V_{n_2}, A_{n_2}, B_{n_2}, U_{n_3}, V_{n_3}, A_{n_3}, B_{n_3})$, where $n_3 = n_1 n_2$ is Diophantine over $O_{\mathbb{Q}, \mathcal{W}}$.***
In a 2009 paper, Eisenträger and Everest extended Poonen's method to prove a theorem concerning sets of complementary primes. If $\mathcal{P}$ is the set of all primes of $\mathbb{Q}$, then two subsets $\mathcal{T}, S \subset \mathcal{P}$ are exactly complementary if $S \cup \mathcal{T} = \mathcal{P}$ and $S \cap \mathcal{T} = \emptyset$.

**Theorem**

*There are exactly complementary recursive sets $S, \mathcal{T} \subset \mathcal{P}$ such that Hilbert's Tenth Problem is undecidable for both rings $O_{\mathbb{Q}, S}$ and $O_{\mathbb{Q}, \mathcal{T}}$.*
Outline

1 Easy or Difficult?
2 Questions: Old and New
   - An Old Question
   - Diophantine Sets and Definitions
   - New Questions
3 Mazur’s Conjectures
   - The Statements of the Conjectures
   - Diophantine Models
   - A Steep Curve
   - What Now?
4 Changing the Object: Rings Big and Small
5 Definability over Small Rings
6 Definability over Big Rings
   - Poonen’s Theorem
   - The Old Plan
   - Putting Two Rings Together
7 Back to the Universal Quantifier
8 And Now for the Big Conjecture
   - Number Fields
   - What We Know Now
   - What We Might Know in the Future
“Diophantine” = “Existentially Definable in the Language of Rings”

If \( A \subset \mathbb{Z} \) is a Diophantine set with a Diophantine definition \( p(t, x_1, \ldots, x_k) \), then

\[
A = \{a \in \mathbb{Z} | \exists x_1, \ldots, \exists x_k \in \mathbb{Z} : p(a, x_1, \ldots, x_k)\}.
\]

In other words \( A \) is defined by an \textit{existential}, i.e. using only existential quantifiers, formula of the first-order language of rings. But what if we allow universal quantifiers?
Fairly Old First-Order Definability Results

**Theorem (Julia Robinson, 1949)**

\[ \mathbb{Z} \text{ is first-order definable over } \mathbb{Q}. \]

**Remark**

Julia Robinson’s formula can be converted to a formula \( (\forall \exists \forall \exists)(F = 0) \) where the \( \forall \)-quantifiers run over a total of 8 variables, and where \( F \) is a polynomial. (Cornelissen and Zahidi, 2007)
Fairly Old First-Order Definability Results

**Theorem (Julia Robinson, 1949)**
\[ \mathbb{Z} \text{ is first-order definable over } \mathbb{Q}. \]

**Remark**
Julia Robinson’s formula can be converted to a formula
\[ (\forall \exists \forall \exists) (F = 0) \]
where the \( \forall \)-quantifiers run over a total of 8 variables, and where \( F \) is a polynomial. (Cornelissen and Zahidi, 2007)

**Theorem (Cornelissen and Zahidi, 2007)**
Assuming a conjecture concerning elliptic curves over \( \mathbb{Q} \), there exists a first-order model of \( \mathbb{Z} \) over \( \mathbb{Q} \) using just one universal quantifier.
Fairly Old First-Order Definability Results

**Theorem (Julia Robinson, 1949)**

\[ \mathbb{Z} \text{ is first-order definable over } \mathbb{Q}. \]

**Remark**

Julia Robinson’s formula can be converted to a formula \((\forall \exists \forall \exists)(F = 0)\) where the \(\forall\)-quantifiers run over a total of 8 variables, and where \(F\) is a polynomial. (Cornelissen and Zahidi, 2007)

**Theorem (Cornelissen and Zahidi, 2007)**

Assuming a conjecture concerning elliptic curves over \(\mathbb{Q}\), there exists a first-order model of \(\mathbb{Z}\) over \(\mathbb{Q}\) using just one universal quantifier.

**Theorem (Poonen, 2008)**

- \(\mathbb{Z}\) is definable over \(\mathbb{Q}\) using just two universal quantifiers in a \(\forall \exists\)-formula.
- For any \(\varepsilon > 0\), there exists a set of rational primes \(\mathcal{W}_Q\) of natural density greater than \(1 - \varepsilon\) such that \(\mathbb{Z}\) is definable using just one quantifier in a \(\forall \exists\)-formula over \(O_{Q, \mathcal{W}_Q}\).
Defining $\mathbb{Z}$ Using Just One Universal Quantifier

Theorem

There exists a set $\mathcal{W}$ of primes of $\mathbb{Q}$ of natural density one such that $\mathbb{Z}$ is first-order definable over $O_{\mathbb{Q},\mathcal{W}}$ using just one universal quantifier in a $\forall\exists$-formula. (S. 2009)
Defining $\mathbb{Z}$ Using Just One Universal Quantifier

**Theorem**

There exists a set $\mathcal{W}$ of primes of $\mathbb{Q}$ of natural density one such that $\mathbb{Z}$ is first-order definable over $\mathbb{O}_{\mathbb{Q},\mathcal{W}}$ using just one universal quantifier in a $\forall \exists$-formula. (S. 2009)

**Theorem**

$\mathbb{Z}$ is first-order definable over $\mathbb{Q}$ using just one $\forall$-quantifier in a $\forall \exists$-formula. (Announced by J. Koenigsman, February 2009)
A Big Project

For which big subrings of $\mathbb{Q}$ is the following true?
For which big subrings of $\mathbb{Q}$ is the following true?

- $\mathbb{Z}$ is existentially definable.
A Big Project

For which big subrings of $\mathbb{Q}$ is the following true?

- $\mathbb{Z}$ is existentially definable.
- $\mathbb{Z}$ has an existential model.
For which big subrings of \( \mathbb{Q} \) is the following true?

- \( \mathbb{Z} \) is existentially definable.
- \( \mathbb{Z} \) has an existential model.
- \( \mathbb{Z} \) is definable using one universal quantifier.
A Big Project

For which big subrings of \( \mathbb{Q} \) is the following true?

- \( \mathbb{Z} \) is existentially definable.
- \( \mathbb{Z} \) has an existential model.
- \( \mathbb{Z} \) is definable using one universal quantifier.

Remark

If we start counting the number of quantifiers we use, definability results over the field will no longer automatically imply the analogous definability results for the subrings. Thus Koenigsman’s result for \( \mathbb{Q} \) does not automatically answer the question about the big subrings in general.
Outline

1 Easy or Difficult?
2 Questions: Old and New
   - An Old Question
   - Diophantine Sets and Definitions
   - New Questions
3 Mazur’s Conjectures
   - The Statements of the Conjectures
   - Diophantine Models
   - A Steep Curve
   - What Now?
4 Changing the Object: Rings Big and Small
5 Definability over Small Rings
6 Definability over Big Rings
   - Poonen’s Theorem
   - The Old Plan
   - Putting Two Rings Together
7 Back to the Universal Quantifier
8 And Now for the Big Conjecture
   - Number Fields
   - What We Know Now
   - What We Might Know in the Future
Some Facts About Number Fields

A number field is a finite extension of \( \mathbb{Q} \).

A totally real number field is a number field all of whose embeddings into its algebraic closure are real.

A ring of integers of a number field is the set of all elements of the number field satisfying monic irreducible polynomials over \( \mathbb{Z} \) or alternatively the integral closure of \( \mathbb{Z} \) in the number field.

Let \( K \) be a number field and let \( W \) be a set of primes of \( K \) (i.e. the set of prime ideals of the ring of integers). Let \( \mathcal{O}_K, W \) be the following subring of \( K \).

\[
\{ x \in K : \text{ord}_p x \geq 0 \ \forall \ p \not\in W \}
\]

If \( W = \emptyset \), then \( \mathcal{O}_K, W = \mathcal{O}_K \) – the ring of integers of \( K \). If \( W \) contains all the primes of \( K \), then \( \mathcal{O}_K, W = K \). If \( W \) is finite, we call the ring small (or the ring of \( W \)-integers). If \( W \) is infinite, we call the ring large, and if the natural density of \( W \) is one, we call the ring “very large.”
A number field is a finite extension of $\mathbb{Q}$.
Some Facts About Number Fields

- A number field is a finite extension of $\mathbb{Q}$.
- A totally real number field is a number field all of whose embeddings into its algebraic closure are real.
Some Facts About Number Fields

- A number field is a finite extension of $\mathbb{Q}$.
- A totally real number field is a number field all of whose embeddings into its algebraic closure are real.
- A ring of integers of a number field is the set of all elements of the number field satisfying monic irreducible polynomials over $\mathbb{Z}$ or alternatively the integral closure of $\mathbb{Z}$ in the number field.
A number field is a finite extension of \( \mathbb{Q} \).

A totally real number field is a number field all of whose embeddings into its algebraic closure are real.

A ring of integers of a number field is the set of all elements of the number field satisfying monic irreducible polynomials over \( \mathbb{Z} \) or alternatively the integral closure of \( \mathbb{Z} \) in the number field.

Let \( K \) be a number field and let \( \mathcal{W} \) be a set of primes of \( K \) (i.e. the set of prime ideals of the ring of integers). Let \( O_{K,\mathcal{W}} \) be the following subring of \( K \).

\[
\{ x \in K : \text{ord}_p x \geq 0 \ \forall p \notin \mathcal{W} \}
\]

If \( \mathcal{W} = \emptyset \), then \( O_{K,\mathcal{W}} = O_K \) – the ring of integers of \( K \). If \( \mathcal{W} \) contains all the primes of \( K \), then \( O_{K,\mathcal{W}} = K \). If \( \mathcal{W} \) is finite, we call the ring small (or the ring of \( \mathcal{W} \)-integers). If \( \mathcal{W} \) is infinite, we call the ring large, and if the natural density of \( \mathcal{W} \) is one, we call the ring “very large”.

The Rings of Integers of Number Fields
The Rings of Integers of Number Fields

Theorem

\( \mathbb{Z} \) is Diophantine and HTP is unsolvable over the rings of integers of the following fields:

- Some extensions of degree 4 of \( \mathbb{Q} \), totally real number fields and their extensions of degree 2. (Denef, 1980 & Denef, Lipshitz, 1978) Note that these fields include all abelian extensions, i.e. the fields whose Galois groups are abelian.
The Rings of Integers of Number Fields

**Theorem**

\( \mathbb{Z} \) is Diophantine and HTP is unsolvable over the rings of integers of the following fields:

- Some extensions of degree 4 of \( \mathbb{Q} \), totally real number fields and their extensions of degree 2. (Denef, 1980 & Denef, Lipshitz, 1978) Note that these fields include all abelian extensions, i.e. the fields whose Galois groups are abelian.
- Number fields with exactly one pair of non-real embeddings (Pheidas, S. 1988)
The Rings of Integers of Number Fields

**Theorem**

$\mathbb{Z}$ is Diophantine and HTP is unsolvable over the rings of integers of the following fields:

- Some extensions of degree 4 of $\mathbb{Q}$, totally real number fields and their extensions of degree 2. (Denef, 1980 & Denef, Lipshitz, 1978) Note that these fields include all abelian extensions, i.e. the fields whose Galois groups are abelian.

- Number fields with exactly one pair of non-real embeddings (Pheidas, S. 1988)

- 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, S. 2003)
The Rings of Integers of Number Fields

Theorem

\(\mathbb{Z}\) is Diophantine and HTP is unsolvable over the rings of integers of the following fields:

- Some extensions of degree 4 of \(\mathbb{Q}\), totally real number fields and their extensions of degree 2. (Denef, 1980 & Denef, Lipshitz, 1978) Note that these fields include all abelian extensions, i.e. the fields whose Galois groups are abelian.
- Number fields with exactly one pair of non-real embeddings (Pheidas, S. 1988)
- 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, S. 2003)
- Any number field \(K\) such that there exists an elliptic curve of rank 1 over \(K\) and an Abelian variety over \(\mathbb{Q}\) keeping its rank over \(K\). (Cornelissen, Pheidas, Zahidi, 2005)
Theorem

Let $K$ be a number field satisfying one of the following conditions:
Theorem

Let \( K \) be a number field satisfying one of the following conditions:
- \( K \) is a totally real field.

Z is Diophantine over \( \mathcal{O}_K \), \( S \).

HTP is unsolvable over \( \mathcal{O}_K \), \( S \).

HTP over Large Subrings of Number Fields

**Theorem**

Let $K$ be a number field satisfying one of the following conditions:

- $K$ is a totally real field.
- $K$ is an extension of degree 2 of a totally real field.
HTP over Large Subrings of Number Fields

Theorem

Let $K$ be a number field satisfying one of the following conditions:

- $K$ is a totally real field.
- $K$ is an extension of degree 2 of a totally real field.
- There exists or an elliptic curve $E$ defined over $\mathbb{Q}$ such that $[E(K) : E(\mathbb{Q})] < \infty$.

Theorem

Let $K$ be a number field satisfying one of the following conditions:

- $K$ is a totally real field.
- $K$ is an extension of degree 2 of a totally real field.
- There exists an elliptic curve $E$ defined over $\mathbb{Q}$ such that $[E(K) : E(\mathbb{Q})] < \infty$.

Let $\varepsilon > 0$ be given. Then there exists a set $S$ of primes of $K$ such that

- The natural density of $S$ is greater than $1 - \frac{1}{[K : \mathbb{Q}]} - \varepsilon$. 
HTP over Large Subrings of Number Fields

Theorem

Let $K$ be a number field satisfying one of the following conditions:

- $K$ is a totally real field.
- $K$ is an extension of degree 2 of a totally real field.
- There exists an elliptic curve $E$ defined over $\mathbb{Q}$ such that $[E(K) : E(\mathbb{Q})] < \infty$.

Let $\varepsilon > 0$ be given. Then there exists a set $S$ of primes of $K$ such that

- The natural density of $S$ is greater than $1 - \frac{1}{[K : \mathbb{Q}]} - \varepsilon$.
- $\mathbb{Z}$ is Diophantine over $O_{K,S}$. 

HTP over Large Subrings of Number Fields

**Theorem**

Let $K$ be a number field satisfying one of the following conditions:

- $K$ is a totally real field.
- $K$ is an extension of degree 2 of a totally real field.
- There exists or an elliptic curve $E$ defined over $\mathbb{Q}$ such that $[E(K) : E(\mathbb{Q})] < \infty$.

Let $\varepsilon > 0$ be given. Then there exists a set $S$ of primes of $K$ such that

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

Theorem

For any number field $K$ with an elliptic curve of rank 1 there exists a set of primes $S$ of natural density 1 such that $\mathbb{Z}$ has a Diophantine model over $O_{K,S}$. (Poonen and S. 2005: constructing model of a model of $\mathbb{Z}$ and S. 2009: multiplication of indices)
Theorem

Suppose $L/K$ is a cyclic extension of prime degree of number fields. If Shafarevich-Tate Conjecture is true for $K$, then there is an elliptic curve $E$ over $K$ with $\text{rank}(E(L)) = \text{rank}(E(K)) = 1$. (Mazur and Rubin, 2009)
Corollary

If Shafarevich-Tate Conjecture is true for all number fields, then the following statements are true.

- \( \mathbb{Z} \) has a Diophantine definition over the ring of integers of any number field \( K \).
Corollary

If Shafarevich-Tate Conjecture is true for all number fields, then the following statements are true.

- \( \mathbb{Z} \) has a Diophantine definition over the ring of integers of any number field \( K \).

- For any number field \( K \) and any \( \varepsilon > 0 \), there exists a set \( S \) of non-archimedean primes of \( K \) such that the natural density of \( S \) is greater than \( 1 - \frac{1}{[K : \mathbb{Q}]} - \varepsilon \) and \( \mathbb{Z} \) is Diophantine over \( \mathcal{O}_{K,S} \).
Corollary

If Shafarevich-Tate Conjecture is true for all number fields, then
the following statements are true.

- \( \mathbb{Z} \) has a Diophantine definition over the ring of integers of any
time number field \( K \).

- For any number field \( K \) and any \( \varepsilon > 0 \), there exists a set \( S \) of
non-archimedean primes of \( K \) such that the natural density of
\( S \) is greater than \( 1 - \frac{1}{[K : \mathbb{Q}]} - \varepsilon \) and \( \mathbb{Z} \) is Diophantine over \( \mathcal{O}_{K,S} \).

- For any number field \( K \), there exists a set of primes \( S \) of
natural density 1 such that \( \mathbb{Z} \) has a Diophantine model over
\( \mathcal{O}_{K,S} \).