Reflections on the work of Pheidas

Konstantinos Kartas

Sorbonne University

PLS 2024

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Diophantine equations

Let $P(X_1, \dots, X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Example

1. $x^2 + y^2 = z^2$. There are infinitely many integer solutions which are precisely the Pythagorean triples:

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Example

1. $x^2 + y^2 = z^2$. There are infinitely many integer solutions which are precisely the Pythagorean triples:

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Example

1. $x^2 + y^2 = z^2$. There are infinitely many integer solutions which are precisely the Pythagorean triples:

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$

(Book X, Euclid 300 BC)

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Example

1. $x^2 + y^2 = z^2$. There are infinitely many integer solutions which are precisely the Pythagorean triples:

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$

   (Book X, Euclid 300 BC)

2. $x^n + y^n = z^n$ and $n > 2$. It has no integer solutions with $xyz \neq 0$. (Wiles 1994)

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Example

1. $x^2 + y^2 = z^2$. There are infinitely many integer solutions which are precisely the Pythagorean triples:
$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$
(Book X, Euclid 300 BC)
2. $x^n + y^n = z^n$ and $n > 2$. It has no integer solutions with $xyz \neq 0$. (Wiles 1994)
[$n = 4$ Fermat (1637),

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Example

1. $x^2 + y^2 = z^2$. There are infinitely many integer solutions which are precisely the Pythagorean triples:
$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$
(Book X, Euclid 300 BC)
2. $x^n + y^n = z^n$ and $n > 2$. It has no integer solutions with $xyz \neq 0$. (Wiles 1994)
[$n = 4$ Fermat (1637), $n = 3$ Euler (1750)]

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Example

1. $x^2 + y^2 = z^2$. There are infinitely many integer solutions which are precisely the Pythagorean triples:

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$

   (Book X, Euclid 300 BC)

2. $x^n + y^n = z^n$ and $n > 2$. It has no integer solutions with $xyz \neq 0$. (Wiles 1994)
   [$n = 4$ Fermat (1637), $n = 3$ Euler (1750)]
3. Does $x^3 + y^3 + z^3 = 33$ have integer solutions?

Diophantine equations

Let $P(X_1, ..., X_n) = 0$ be a polynomial equation with integer coefficients.

Questions:

1. Is it solvable in $\mathbb{Z}$?
2. If yes, what does the solution set look like? For instance, is it finite or infinite?

Example

1. $x^2 + y^2 = z^2$. There are infinitely many integer solutions which are precisely the Pythagorean triples:

   $$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$

   (Book X, Euclid 300 BC)
2. $x^n + y^n = z^n$ and $n > 2$. It has no integer solutions with $xyz \neq 0$. (Wiles 1994)
   [$n = 4$ Fermat (1637), $n = 3$ Euler (1750)]
3. Does $x^3 + y^3 + z^3 = 33$ have integer solutions? No one knows.

Hilbert's tenth problem (1900)

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, \ldots, X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation.

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation.
(e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation. (e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation.
(e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation. (e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ *is undecidable in* $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation.
(e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R)

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation. (e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R) (e.g., instead of $\mathbb{Z}$, consider $\mathbb{C}$

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation.
(e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ *is undecidable in* $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.
There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R)
   (e.g., instead of $\mathbb{Z}$, consider $\mathbb{C}$ or $\mathbb{R}$

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation.
(e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R)
   (e.g., instead of $\mathbb{Z}$, consider $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Q}_p$

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation. (e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R) (e.g., instead of $\mathbb{Z}$, consider $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Q}_p$ or $\mathbb{Q}$ (**!**)

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation. (e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R) (e.g., instead of $\mathbb{Z}$, consider $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Q}_p$ or $\mathbb{Q}$ (**!**))

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation. (e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R) (e.g., instead of $\mathbb{Z}$, consider $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Q}_p$ or $\mathbb{Q}$ (**!**))
2. Consider more general sentences (not just existential ones). (It was already known in the '30s that $Th(\mathbb{Z})$ is undecidable, Gödel, Church, Turing.)

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation.
(e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R)
   (e.g., instead of $\mathbb{Z}$, consider $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Q}_p$ or $\mathbb{Q}$ (**!**))
2. Consider more general sentences (not just existential ones).
   (It was already known in the '30s that $Th(\mathbb{Z})$ is undecidable, Gödel, Church, Turing.)
3. Change the language.

Hilbert's tenth problem (1900)

H10 Problem: Find an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with integer coefficients is solvable in $\mathbb{Z}$.

One can also consider systems but this reduces to one equation. (e.g., $P_1 = P_2 = 0 \iff P_1^2 + P_2^2 = 0$)

Theorem (DPRM '70)

No such algorithm exists. Equivalently, $Th_{\exists^+}(\mathbb{Z})$ is undecidable in $L_{rings} = \{+, \cdot, 0, 1\}$.

This would certainly come as a surprise to Hilbert.

There are (at least) three possible ways of extending H10 problem:

1. Change the domain where we look for solutions. (H10/R)
   (e.g., instead of $\mathbb{Z}$, consider $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Q}_p$ or $\mathbb{Q}$ (**!**))
2. Consider more general sentences (not just existential ones).
   (It was already known in the '30s that $Th(\mathbb{Z})$ is undecidable, Gödel, Church, Turing.)
3. Change the language.
   (For instance, $(\mathbb{Z}, +)$ is decidable.)

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ *with rational coefficients is solvable in* $\mathbb{Q}$*?*

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ *with rational coefficients is solvable in* $\mathbb{Q}$*?*

Remarks:

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, \ldots, X_n) = 0$ *with rational coefficients is solvable in* $\mathbb{Q}$*?*

Remarks:

- Most experts expect the answer to be negative (just as H10/$\mathbb{Z}$).

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ *with rational coefficients is solvable in* $\mathbb{Q}$*?*

Remarks:

- Most experts expect the answer to be negative (just as H10/$\mathbb{Z}$).
- It sounds like this should follow easily from the case over $\mathbb{Z}$ by simply "clearing denominators" but this is not the case!

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, \ldots, X_n) = 0$ *with rational coefficients is solvable in* $\mathbb{Q}$*?*

Remarks:

- Most experts expect the answer to be negative (just as H10/$\mathbb{Z}$).
- It sounds like this should follow easily from the case over $\mathbb{Z}$ by simply "clearing denominators" but this is not the case!
- Towards an answer to H10/$\mathbb{Q}$, it may be instructive to look at fields whose arithmetic is similar to $\mathbb{Q}$.

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with rational coefficients is solvable in $\mathbb{Q}$?

Remarks:

- Most experts expect the answer to be negative (just as H10/$\mathbb{Z}$).
- It sounds like this should follow easily from the case over $\mathbb{Z}$ by simply "clearing denominators" but this is not the case!
- Towards an answer to H10/$\mathbb{Q}$, it may be instructive to look at fields whose arithmetic is similar to $\mathbb{Q}$.
- There is a classical analogy between $\mathbb{Q}$ and fields of rational functions $F(t)$ (F a field),

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, \ldots, X_n) = 0$ *with rational coefficients is solvable in* $\mathbb{Q}$*?*

Remarks:

- Most experts expect the answer to be negative (just as H10/$\mathbb{Z}$).
- It sounds like this should follow easily from the case over $\mathbb{Z}$ by simply "clearing denominators" but this is not the case!
- Towards an answer to H10/$\mathbb{Q}$, it may be instructive to look at fields whose arithmetic is similar to $\mathbb{Q}$.
- There is a classical analogy between $\mathbb{Q}$ and fields of rational functions $F(t)$ (F a field), whose elements are of the form $f(t)/g(t)$, where $f(t), g(t) \in F[t]$ and $g(t) \not\equiv 0$.

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with rational coefficients is solvable in $\mathbb{Q}$?

Remarks:

- Most experts expect the answer to be negative (just as H10/$\mathbb{Z}$).
- It sounds like this should follow easily from the case over $\mathbb{Z}$ by simply "clearing denominators" but this is not the case!
- Towards an answer to H10/$\mathbb{Q}$, it may be instructive to look at fields whose arithmetic is similar to $\mathbb{Q}$.
- There is a classical analogy between $\mathbb{Q}$ and fields of rational functions $F(t)$ (F a field), whose elements are of the form $f(t)/g(t)$, where $f(t), g(t) \in F[t]$ and $g(t) \neq 0$.

Pheidas did some work on H10/$\mathbb{Q}$

Pheidas' journey towards Ithaka (H10/$\mathbb{Q}$)

Perhaps the prominent open problem in the area is H10/$\mathbb{Q}$:

Problem

Is there an algorithm to decide whether a given polynomial equation $P(X_1, ..., X_n) = 0$ with rational coefficients is solvable in $\mathbb{Q}$?

Remarks:

- Most experts expect the answer to be negative (just as H10/$\mathbb{Z}$).
- It sounds like this should follow easily from the case over $\mathbb{Z}$ by simply "clearing denominators" but this is not the case!
- Towards an answer to H10/$\mathbb{Q}$, it may be instructive to look at fields whose arithmetic is similar to $\mathbb{Q}$.
- There is a classical analogy between $\mathbb{Q}$ and fields of rational functions $F(t)$ (F a field), whose elements are of the form $f(t)/g(t)$, where $f(t), g(t) \in F[t]$ and $g(t) \neq 0$.

Pheidas did some work on H10/$\mathbb{Q}$ but the most definitive and striking results he obtained were about function fields.

Function Field Analogy (A. Weil '40)

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers".

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers".
   ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers".
   ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

    3.1 The prime 2 gives rise to $| \ |_2$:

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

    3.1 The prime 2 gives rise to $| \ |_2$: To compute $|m|_2$, write $m = 2^s \cdot n$ with $2 \nmid n$.

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers".
   ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

   3.1 The prime 2 gives rise to $|\ |_2$: To compute $|m|_2$, write $m = 2^s \cdot n$ with $2 \nmid n$. Then $|m|_2 = 1/2^s$.

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

   3.1 The prime 2 gives rise to $|\ |_2$: To compute $|m|_2$, write $m = 2^s \cdot n$ with $2 \nmid n$. Then $|m|_2 = 1/2^s$. The completion of $\mathbb{Q}$ w.r.t. $|\ |_2$ is denoted by $\mathbb{Q}_2$.

   3.2 The 'prime' t gives rise to $|\ |_t$:

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

   3.1 The prime 2 gives rise to $|\ |_2$: To compute $|m|_2$, write $m = 2^s \cdot n$ with $2 \nmid n$. Then $|m|_2 = 1/2^s$. The completion of $\mathbb{Q}$ w.r.t. $|\ |_2$ is denoted by $\mathbb{Q}_2$.

   3.2 The 'prime' t gives rise to $|\ |_t$: To compute $|f|_t$, write $f = t^s \cdot g$ with $t \nmid g$.

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers".
   ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

   3.1 The prime 2 gives rise to $|\ |_2$: To compute $|m|_2$, write $m = 2^s \cdot n$ with $2 \nmid n$. Then $|m|_2 = 1/2^s$. The completion of $\mathbb{Q}$ w.r.t. $|\ |_2$ is denoted by $\mathbb{Q}_2$.

   3.2 The 'prime' t gives rise to $|\ |_t$: To compute $|f|_t$, write $f = t^s \cdot g$ with $t \nmid g$. Then $|f|_t = 1/2^s$.

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).
   - 3.1 The prime 2 gives rise to $|\ |_2$: To compute $|m|_2$, write $m = 2^s \cdot n$ with $2 \nmid n$. Then $|m|_2 = 1/2^s$. The completion of $\mathbb{Q}$ w.r.t. $|\ |_2$ is denoted by $\mathbb{Q}_2$.
   - 3.2 The 'prime' t gives rise to $|\ |_t$: To compute $|f|_t$, write $f = t^s \cdot g$ with $t \nmid g$. Then $|f|_t = 1/2^s$. We write $s = ord_t(x)$.

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

    3.1 The prime 2 gives rise to $|\ |_2$: To compute $|m|_2$, write $m = 2^s \cdot n$ with $2 \nmid n$. Then $|m|_2 = 1/2^s$. The completion of $\mathbb{Q}$ w.r.t. $|\ |_2$ is denoted by $\mathbb{Q}_2$.
    3.2 The 'prime' t gives rise to $|\ |_t$: To compute $|f|_t$, write $f = t^s \cdot g$ with $t \nmid g$. Then $|f|_t = 1/2^s$. We write $s = ord_t(x)$. The completion of $\mathbb{F}_p(t)$ w.r.t. $ord_t(x)$ is denoted by $\mathbb{F}_p((t))$.

Function Field Analogy (A. Weil '40)

$$\mathbb{Q} \quad \text{vs} \quad \mathbb{F}_p(t)$$

These two fields are remarkably similar:

1. They both have a notion of a "ring of integers". ($\mathbb{Z} \subseteq \mathbb{Q}$ vs $\mathbb{F}_p[t] \subseteq \mathbb{F}_p(t)$.)
2. Both rings have a notion of a "prime" element and satisfy a version of the fundamental theorem of arithmetic.
3. Each "prime" defines an absolute value and the completed field w.r.t. that absolute value is locally compact (just like $\mathbb{R}$).

    3.1 The prime 2 gives rise to $|\ |_2$: To compute $|m|_2$, write $m = 2^s \cdot n$ with $2 \nmid n$. Then $|m|_2 = 1/2^s$. The completion of $\mathbb{Q}$ w.r.t. $|\ |_2$ is denoted by $\mathbb{Q}_2$.

    3.2 The 'prime' t gives rise to $|\ |_t$: To compute $|f|_t$, write $f = t^s \cdot g$ with $t \nmid g$. Then $|f|_t = 1/2^s$. We write $s = ord_t(x)$. The completion of $\mathbb{F}_p(t)$ w.r.t. $ord_t(x)$ is denoted by $\mathbb{F}_p(\!(t)\!)$.

Remark: Properties (1)-(3) in fact "axiomatize" completely these fields. (Artin-Whaples '45)

Hilbert's tenth problem over function fields

Hilbert's tenth problem over function fields

Theorem (Pheidas '91 for $p > 2$, Videla '94 for $p = 2$)

Hilbert's tenth problem over $\mathbb{F}_p(t)$ is undecidable.

Hilbert's tenth problem over function fields

Theorem (Pheidas '91 for $p > 2$, Videla '94 for $p = 2$)

Hilbert's tenth problem over $\mathbb{F}_p(t)$ is undecidable. Equivalently, the existential theory of $\mathbb{F}_p(t)$ is undecidable in the language of rings with a constant for t.

Hilbert's tenth problem over function fields

Theorem (Pheidas '91 for $p > 2$, Videla '94 for $p = 2$)

Hilbert's tenth problem over $\mathbb{F}_p(t)$ *is undecidable. Equivalently, the existential theory of* $\mathbb{F}_p(t)$ *is undecidable in the language of rings with a constant for* t.

Why is this result important?

Hilbert's tenth problem over function fields

Theorem (Pheidas '91 for $p > 2$, Videla '94 for $p = 2$)

Hilbert's tenth problem over $\mathbb{F}_p(t)$ is undecidable. Equivalently, the existential theory of $\mathbb{F}_p(t)$ is undecidable in the language of rings with a constant for t.

Why is this result important?

- It is perhaps the strongest piece of evidence that H10 over $\mathbb{Q}$ should be undecidable.

Hilbert's tenth problem over function fields

Theorem (Pheidas '91 for $p > 2$, Videla '94 for $p = 2$)

Hilbert's tenth problem over $\mathbb{F}_p(t)$ is undecidable. Equivalently, the existential theory of $\mathbb{F}_p(t)$ is undecidable in the language of rings with a constant for t.

Why is this result important?

- It is perhaps the strongest piece of evidence that H10 over $\mathbb{Q}$ should be undecidable.

There is also a uniform version which is even more suggestive:

Hilbert's tenth problem over function fields

Theorem (Pheidas '91 for $p > 2$, Videla '94 for $p = 2$)

Hilbert's tenth problem over $\mathbb{F}_p(t)$ is undecidable. Equivalently, the existential theory of $\mathbb{F}_p(t)$ is undecidable in the language of rings with a constant for t.

Why is this result important?

- It is perhaps the strongest piece of evidence that H10 over $\mathbb{Q}$ should be undecidable.

There is also a uniform version which is even more suggestive:

Theorem (Pasten-Pheidas-Vidaux '13)

There is no algorithm to decide whether a system of polynomial equations with coefficients in $\mathbb{Z}[t]$ has a solution in $\mathbb{F}_p[t]$ for all but finitely many p.

Hilbert's tenth problem over function fields

Theorem (Pheidas '91 for $p > 2$, Videla '94 for $p = 2$)

Hilbert's tenth problem over $\mathbb{F}_p(t)$ is undecidable. Equivalently, the existential theory of $\mathbb{F}_p(t)$ is undecidable in the language of rings with a constant for t.

Why is this result important?

- It is perhaps the strongest piece of evidence that H10 over $\mathbb{Q}$ should be undecidable.

There is also a uniform version which is even more suggestive:

Theorem (Pasten-Pheidas-Vidaux '13)

There is no algorithm to decide whether a system of polynomial equations with coefficients in $\mathbb{Z}[t]$ has a solution in $\mathbb{F}_p[t]$ for all but finitely many p.

cf. (Ax 1967)
There *is* an algorithm to decide whether a system of polynomial equations with coefficients in $\mathbb{Z}$ has a solution in $\mathbb{F}_p$ for all but finitely many primes p.

H10 over function fields is undecidable: The proof

Theorem (Pheidas '91 for $p > 2$, Videla '94 for $p = 2$)

Hilbert's tenth problem over $\mathbb{F}_p(t)$ is undecidable.

Pheidas encodes Hilbert's 10th problem over $\mathbb{Z}$ in an ingenious way.

Key steps in the proof:

1. We identify $\mathbb{Z} = \{ord_t(x) : x \in \mathbb{F}_p(t)\}$.
   (The relation $ord_t(x) \geq 0$ is $\exists^+$-definable, so we can encode the $\exists^+$-theory of $(\mathbb{Z}, <)$.)
2. Note that $ord_t(xy) = ord_t(x) + ord_t(y)$, so we can encode the $\exists^+$-theory of $(\mathbb{Z}, +, <)$. How to encode multiplication?
3. Pheidas first encodes the relation
   $$m \mid_p n :\iff n = p^s \cdot m \text{ for some } s \in \mathbb{N}$$
   (By showing that "$x = y^{p^s}$" is $\exists^+$-definable in $\mathbb{F}_p(t)$.)
4. In previous work, Pheidas showed that multiplication is $\exists^+$-definable in $(\mathbb{Z}, +, <, \mid_p)$.
5. Thus, we can encode the $\exists^+$-theory of $(\mathbb{Z}, +, \cdot)$, which is undecidable by the DPRM theorem.

Hilbert's tenth problem over $\mathbb{F}_p((t))$

Does the situation improve if we replace $\mathbb{F}_p(t)$ with $\mathbb{F}_p((t))$?

Problem

Is Hilbert's tenth problem over $\mathbb{F}_p((t))$ is decidable? Equivalently, is $Th_\exists(\mathbb{F}_p((t)))$ decidable in L_{rings} with a constant for t?

Hilbert's tenth problem over $\mathbb{F}_p((t))$

Does the situation improve if we replace $\mathbb{F}_p(t)$ with $\mathbb{F}_p((t))$?

Problem

Is Hilbert's tenth problem over $\mathbb{F}_p((t))$ is decidable? Equivalently, is $Th_\exists(\mathbb{F}_p((t)))$ decidable in L_{rings} with a constant for t?

Note:

Hilbert's 10th problem over $\mathbb{C}((t))$ is decidable

Hilbert's tenth problem over $\mathbb{F}_p((t))$

Does the situation improve if we replace $\mathbb{F}_p(t)$ with $\mathbb{F}_p((t))$?

Problem

Is Hilbert's tenth problem over $\mathbb{F}_p((t))$ is decidable? Equivalently, is $Th_\exists(\mathbb{F}_p((t)))$ decidable in L_{rings} with a constant for t?

Note:

Hilbert's 10th problem over $\mathbb{C}((t))$ is decidable and also the full first-order theory of $\mathbb{C}((t))$. (Ax-Kochen/Ershov '66)

Theorem (Denef-Schoutens '03, K. '22, Anscombe-Dittmann-Fehm '23)

H10 over $\mathbb{F}_p((t))$ is decidable, if one assumes resolution of singularities

Hilbert's tenth problem over $\mathbb{F}_p((t))$

Does the situation improve if we replace $\mathbb{F}_p(t)$ with $\mathbb{F}_p((t))$?

Problem

Is Hilbert's tenth problem over $\mathbb{F}_p((t))$ is decidable? Equivalently, is $Th_\exists(\mathbb{F}_p((t)))$ decidable in L_{rings} with a constant for t?

Note:

Hilbert's 10th problem over $\mathbb{C}((t))$ is decidable and also the full first-order theory of $\mathbb{C}((t))$. (Ax-Kochen/Ershov '66)

Theorem (Denef-Schoutens '03, K. '22, Anscombe-Dittmann-Fehm '23)

H10 over $\mathbb{F}_p((t))$ is decidable, if one assumes resolution of singularities (or some weak local version of it).

Hilbert's tenth problem over $\mathbb{F}_p((t))$

Does the situation improve if we replace $\mathbb{F}_p(t)$ with $\mathbb{F}_p((t))$?

Problem

Is Hilbert's tenth problem over $\mathbb{F}_p((t))$ is decidable? Equivalently, is $Th_\exists(\mathbb{F}_p((t)))$ decidable in L_{rings} with a constant for t?

Note:

Hilbert's 10th problem over $\mathbb{C}((t))$ is decidable and also the full first-order theory of $\mathbb{C}((t))$. (Ax-Kochen/Ershov '66)

Theorem (Denef-Schoutens '03, K. '22, Anscombe-Dittmann-Fehm '23)

H10 over $\mathbb{F}_p((t))$ is decidable, if one assumes resolution of singularities (or some weak local version of it).

Theorem (Pheidas '87)

The existential theory of $\mathbb{F}_p((t))$ is undecidable in the language of rings with a constant for t and a predicate for $P = \{1, t, t^2, \ldots\}$.

Hilbert's tenth problem over $\mathbb{F}_p((t))$

Does the situation improve if we replace $\mathbb{F}_p(t)$ with $\mathbb{F}_p((t))$?

Problem

Is Hilbert's tenth problem over $\mathbb{F}_p((t))$ is decidable? Equivalently, is $Th_\exists(\mathbb{F}_p((t)))$ decidable in L_{rings} with a constant for t?

Note:

Hilbert's 10th problem over $\mathbb{C}((t))$ is decidable and also the full first-order theory of $\mathbb{C}((t))$. (Ax-Kochen/Ershov '66)

Theorem (Denef-Schoutens '03, K. '22, Anscombe-Dittmann-Fehm '23)

H10 over $\mathbb{F}_p((t))$ is decidable, if one assumes resolution of singularities (or some weak local version of it).

Theorem (Pheidas '87)

The existential theory of $\mathbb{F}_p((t))$ is undecidable in the language of rings with a constant for t and a predicate for $P = \{1, t, t^2, ...\}$.

See Leo Gitin's talk for more details.