Hilbert's 10th Problem

Warwick Postgraduate Seminar

Robin Visser
Mathematics Institute
University of Warwick

26 October 2022

Hilbert's 10th problem

In 1900, at the second ICM, David Hilbert presented a list of 23 unsolved problems. This was his 10th problem:

Hilbert's 10th problem

In 1900, at the second ICM, David Hilbert presented a list of 23 unsolved problems. This was his 10th problem:

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Hilbert's 10th problem

In 1900, at the second ICM, David Hilbert presented a list of 23 unsolved problems. This was his 10th problem:

> **10. Determination of the Solvability of a Diophantine Equation.**
>
> Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Hilbert's 10th problem

In 1900, at the second ICM, David Hilbert presented a list of 23 unsolved problems. This was his 10th problem:

> **10. Determination of the Solvability of a Diophantine Equation.**
>
> Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Hilbert (1900)

Find an algorithm that decides whether any given polynomial equation $p(x_1, \ldots, x_n) = 0$ over the integers has an integral solution $x_1, \ldots, x_n \in \mathbb{Z}$.

Examples

Examples

- $x^2 = 61y^2 + 1$

Examples

- $x^2 = 61y^2 + 1$
  $x = 1766319049, \quad y = 226153980$ (solved by Brahmagupta 628)

Examples

- $x^2 = 61y^2 + 1$
  $x = 1766319049, \quad y = 226153980$ (solved by Brahmagupta 628)
- $x^4 + y^4 = z^4$ (no solutions if $xyz \neq 0$, proven by Fermat 1637)

Examples

- $x^2 = 61y^2 + 1$
  $x = 1766319049, \quad y = 226153980$ (solved by Brahmagupta 628)
- $x^4 + y^4 = z^4$ (no solutions if $xyz \neq 0$, proven by Fermat 1637)
- $x^3 + y^3 + z^3 = 42$

Examples

- $x^2 = 61y^2 + 1$
  $x = 1766319049, \quad y = 226153980$ (solved by Brahmagupta 628)
- $x^4 + y^4 = z^4$ (no solutions if $xyz \neq 0$, proven by Fermat 1637)
- $x^3 + y^3 + z^3 = 42$ (solution found by Booker, Sutherland, 2019)
  $x = -80538738812075974, \quad y = 80435758145817515, \quad z = 12602123297335631$

Examples

- $x^2 = 61y^2 + 1$
  $x = 1766319049, \quad y = 226153980$ (solved by Brahmagupta 628)
- $x^4 + y^4 = z^4$ (no solutions if $xyz \neq 0$, proven by Fermat 1637)
- $x^3 + y^3 + z^3 = 42$ (solution found by Booker, Sutherland, 2019)
  $x = -80538738812075974, \quad y = 80435758145817515, \quad z = 12602123297335631$
- Archimedes Cattle problem:

  $W = \frac{5}{6}X + Z, \quad X = \frac{9}{20}Y + Z, \quad Y = \frac{13}{42}W + Z, \quad w = \frac{7}{12}(X + x), \quad W + X = a^2,$
  $x = \frac{9}{20}(Y + y), \quad y = \frac{11}{30}(Z + z), \quad z = \frac{13}{42}(W + w), \quad Y + Z = \frac{1}{2}b(b + 1)$

Examples

- $x^2 = 61y^2 + 1$
  $x = 1766319049, \quad y = 226153980$ (solved by Brahmagupta 628)
- $x^4 + y^4 = z^4$ (no solutions if $xyz \neq 0$, proven by Fermat 1637)
- $x^3 + y^3 + z^3 = 42$ (solution found by Booker, Sutherland, 2019)
  $x = -80538738812075974, \quad y = 80435758145817515, \quad z = 12602123297335631$
- Archimedes Cattle problem:

  $W = \frac{5}{6}X + Z, \quad X = \frac{9}{20}Y + Z, \quad Y = \frac{13}{42}W + Z, \quad w = \frac{7}{12}(X + x), \quad W + X = a^2,$
  $x = \frac{9}{20}(Y + y), \quad y = \frac{11}{30}(Z + z), \quad z = \frac{13}{42}(W + w), \quad Y + Z = \frac{1}{2}b(b + 1)$

  $W + X + Y + Z + w + x + y + z \approx 7.76 \times 10^{206544}$ (solved by Amthor 1880)

Examples

Open problems:

- Does there exist $x, y, z \in \mathbb{Z}$ such that $x^3 + y^3 + z^3 = 114$?

Examples

Open problems:

- Does there exist $x, y, z \in \mathbb{Z}$ such that $x^3 + y^3 + z^3 = 114$?
- Does there exist $a, b, c, d, e, f \in \mathbb{Z}_{>0}$ such that $a^6 + b^6 + c^6 + d^6 + e^6 = f^6$?

Examples

Open problems:

- Does there exist $x, y, z \in \mathbb{Z}$ such that $x^3 + y^3 + z^3 = 114$?
- Does there exist $a, b, c, d, e, f \in \mathbb{Z}_{>0}$ such that $a^6 + b^6 + c^6 + d^6 + e^6 = f^6$?
- **Erdős–Straus conjecture**: For every n, does there exist $x, y, z \in \mathbb{Z}_{>0}$ such that $4xyz = n(xy + xz + yz)$?

Examples

Open problems:

- Does there exist $x, y, z \in \mathbb{Z}$ such that $x^3 + y^3 + z^3 = 114$?
- Does there exist $a, b, c, d, e, f \in \mathbb{Z}_{>0}$ such that $a^6 + b^6 + c^6 + d^6 + e^6 = f^6$?
- **Erdős–Straus conjecture**: For every n, does there exist $x, y, z \in \mathbb{Z}_{>0}$ such that $4xyz = n(xy + xz + yz)$?
- **Perfect Cuboid:** Does there exist $a, b, c, d, e, f, g \in \mathbb{Z}$ such that

$$a^2 + b^2 = d^2, \quad a^2 + c^2 = e^2, \quad b^2 + c^2 = f^2, \quad a^2 + b^2 + c^2 = g^2$$

Examples

Open problems:

- Does there exist $x, y, z \in \mathbb{Z}$ such that $x^3 + y^3 + z^3 = 114$?
- Does there exist $a, b, c, d, e, f \in \mathbb{Z}_{>0}$ such that $a^6 + b^6 + c^6 + d^6 + e^6 = f^6$?
- **Erdős–Straus conjecture**: For every n, does there exist $x, y, z \in \mathbb{Z}_{>0}$ such that $4xyz = n(xy + xz + yz)$?
- **Perfect Cuboid:** Does there exist $a, b, c, d, e, f, g \in \mathbb{Z}$ such that

$$a^2 + b^2 = d^2, \quad a^2 + c^2 = e^2, \quad b^2 + c^2 = f^2, \quad a^2 + b^2 + c^2 = g^2$$

Diophantine equations are hard!

Hilbert's 10th problem

Remarks:

- A polynomial $P(x_1, \ldots, x_n) = 0$ has a solution over the integers if and only if $P(x_1 - z_1, \ldots, x_n - z_n) = 0$ has a solution over the naturals.

Hilbert's 10th problem

Remarks:

- A polynomial $P(x_1, \ldots, x_n) = 0$ has a solution over the integers if and only if $P(x_1 - z_1, \ldots, x_n - z_n) = 0$ has a solution over the naturals.
- A polynomial $P(x_1, \ldots, x_n) = 0$ has a solution over the naturals if and only if $P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \ldots, w_n^2 + x_n^2 + y_n^2 + z_n^2) = 0$ has a solution over the integers, by Lagrange's four squares theorem.

Hilbert's 10th problem

Remarks:

- A polynomial $P(x_1, \ldots, x_n) = 0$ has a solution over the integers if and only if $P(x_1 - z_1, \ldots, x_n - z_n) = 0$ has a solution over the naturals.
- A polynomial $P(x_1, \ldots, x_n) = 0$ has a solution over the naturals if and only if $P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \ldots, w_n^2 + x_n^2 + y_n^2 + z_n^2) = 0$ has a solution over the integers, by Lagrange's four squares theorem.
- A system of polynomial equations $P_1(x_1, \ldots, x_n) = \cdots = P_n(x_1, \ldots, x_n) = 0$ has a solution if and only if $P_1(x_1, \ldots, x_n)^2 + \cdots + P_n(x_1, \ldots, x_n)^2 = 0$ has a solution.

Diophantine sets

Convention: $\mathbb{N} = \{0, 1, 2, \dots\}$.

Definition

Let $n \in \mathbb{N}$. A set $S \subset \mathbb{N}^n$ is **Diophantine** if there exists $m \in \mathbb{N}$ and a polynomial $P(x_1, \dots, x_n, y_1, \dots, y_m)$ with integer coefficients such that

$$(x_1, \dots, x_n) \in S \iff \exists y_1, \dots, y_m \in \mathbb{N}, P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$$

We say that P *represents* S.

Diophantine sets

Convention: $\mathbb{N} = \{0, 1, 2, \dots\}$.

Definition

Let $n \in \mathbb{N}$. A set $S \subset \mathbb{N}^n$ is **Diophantine** if there exists $m \in \mathbb{N}$ and a polynomial $P(x_1, \dots, x_n, y_1, \dots, y_m)$ with integer coefficients such that

$$(x_1, \dots, x_n) \in S \iff \exists y_1, \dots, y_m \in \mathbb{N}, P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$$

We say that P *represents* S.

Examples:

- Any finite set $S = \{s_1, \dots, s_k\}$. Take $P = (x - s_1) \cdots (x - s_k)$.

Diophantine sets

Convention: $\mathbb{N} = \{0, 1, 2, \dots\}$.

Definition

Let $n \in \mathbb{N}$. A set $S \subset \mathbb{N}^n$ is **Diophantine** if there exists $m \in \mathbb{N}$ and a polynomial $P(x_1, \dots, x_n, y_1, \dots, y_m)$ with integer coefficients such that

$$(x_1, \dots, x_n) \in S \iff \exists y_1, \dots, y_m \in \mathbb{N}, P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$$

We say that P *represents* S.

Examples:

- Any finite set $S = \{s_1, \dots, s_k\}$. Take $P = (x - s_1) \cdots (x - s_k)$.
- Even numbers: $S = \{0, 2, 4, 6, \dots\}$. Take $P = x - 2y$.

Diophantine sets

Convention: $\mathbb{N} = \{0, 1, 2, \dots\}$.

Definition

Let $n \in \mathbb{N}$. A set $S \subset \mathbb{N}^n$ is **Diophantine** if there exists $m \in \mathbb{N}$ and a polynomial $P(x_1, \dots, x_n, y_1, \dots, y_m)$ with integer coefficients such that

$$(x_1, \dots, x_n) \in S \iff \exists y_1, \dots, y_m \in \mathbb{N}, P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$$

We say that P *represents* S.

Examples:

- Any finite set $S = \{s_1, \dots, s_k\}$. Take $P = (x - s_1) \cdots (x - s_k)$.
- Even numbers: $S = \{0, 2, 4, 6, \dots\}$. Take $P = x - 2y$.
- Composite numbers $S = \{4, 6, 8, 9, 10, \dots, \}$. Take $P = x - (y_1 + 2)(y_2 + 2)$.

Diophantine sets

Convention: $\mathbb{N} = \{0, 1, 2, \dots\}$.

Definition

Let $n \in \mathbb{N}$. A set $S \subset \mathbb{N}^n$ is **Diophantine** if there exists $m \in \mathbb{N}$ and a polynomial $P(x_1, \dots, x_n, y_1, \dots, y_m)$ with integer coefficients such that

$$(x_1, \dots, x_n) \in S \iff \exists y_1, \dots, y_m \in \mathbb{N}, P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$$

We say that P *represents* S.

Examples:

- Any finite set $S = \{s_1, \dots, s_k\}$. Take $P = (x - s_1) \cdots (x - s_k)$.
- Even numbers: $S = \{0, 2, 4, 6, \dots\}$. Take $P = x - 2y$.
- Composite numbers $S = \{4, 6, 8, 9, 10, \dots, \}$. Take $P = x - (y_1 + 2)(y_2 + 2)$.
- Non-powers of 2: $S = \{0, 3, 5, 6, \dots\}$. Take $P = x - y_1(2y_2 + 3)$.

Diophantine sets

Convention: $\mathbb{N} = \{0, 1, 2, \dots\}$.

Definition

Let $n \in \mathbb{N}$. A set $S \subset \mathbb{N}^n$ is **Diophantine** if there exists $m \in \mathbb{N}$ and a polynomial $P(x_1, \dots, x_n, y_1, \dots, y_m)$ with integer coefficients such that

$$(x_1, \dots, x_n) \in S \iff \exists y_1, \dots, y_m \in \mathbb{N}, P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$$

We say that P *represents* S.

Examples:

- Any finite set $S = \{s_1, \dots, s_k\}$. Take $P = (x - s_1) \cdots (x - s_k)$.
- Even numbers: $S = \{0, 2, 4, 6, \dots\}$. Take $P = x - 2y$.
- Composite numbers $S = \{4, 6, 8, 9, 10, \dots, \}$. Take $P = x - (y_1 + 2)(y_2 + 2)$.
- Non-powers of 2: $S = \{0, 3, 5, 6, \dots\}$. Take $P = x - y_1(2y_2 + 3)$.

What about prime numbers: $S = \{2, 3, 5, 7, \dots\}$, or powers of 2: $S = \{1, 2, 4, 8, \dots\}$?

Diophantine sets

Relation examples:

- Equality $x = y$: Take $P = x - y$

Diophantine sets

Relation examples:

- Equality $x = y$: Take $P = x - y$
- Relation $x \leq y$: Take $P = x + z - y$.

Diophantine sets

Relation examples:

- Equality $x = y$: Take $P = x - y$
- Relation $x \leq y$: Take $P = x + z - y$.
- Divisibility $x|y$: Take $P = xz - y$

Diophantine sets

Relation examples:

- Equality $x = y$: Take $P = x - y$
- Relation $x \leq y$: Take $P = x + z - y$.
- Divisibility $x|y$: Take $P = xz - y$
- Congruence $x \equiv y \pmod{m}$: Take $P = (x - y - mz)(y - x - mz)$

Diophantine sets

Lemma

Let $D_1, D_2 \subset \mathbb{N}^n$ be Diophantine sets. Then $D_1 \cup D_2$ and $D_1 \cap D_2$ are Diophantine sets.

Diophantine sets

Lemma

Let $D_1, D_2 \subset \mathbb{N}^n$ be Diophantine sets. Then $D_1 \cup D_2$ and $D_1 \cap D_2$ are Diophantine sets.

Proof: Let P represent D_1, and let Q represent D_2. Then PQ represents $D_1 \cup D_2$, and $P^2 + Q^2$ represents $D_1 \cap D_2$.

Diophantine sets

Lemma

Let $D_1, D_2 \subset \mathbb{N}^n$ be Diophantine sets. Then $D_1 \cup D_2$ and $D_1 \cap D_2$ are Diophantine sets.

Proof: Let P represent D_1, and let Q represent D_2. Then PQ represents $D_1 \cup D_2$, and $P^2 + Q^2$ represents $D_1 \cap D_2$.

Lemma

Let $D_1 \in \mathbb{N}^{n+1}$. Then the set $D_2 := \{(x_1, \ldots, x_n) \in \mathbb{N}^n : \exists z \, (z, x_1, \ldots, x_n) \in D_1\}$ is Diophantine.

Diophantine sets

Lemma

Let $D_1, D_2 \subset \mathbb{N}^n$ be Diophantine sets. Then $D_1 \cup D_2$ and $D_1 \cap D_2$ are Diophantine sets.

Proof: Let P represent D_1, and let Q represent D_2. Then PQ represents $D_1 \cup D_2$, and $P^2 + Q^2$ represents $D_1 \cap D_2$.

Lemma

Let $D_1 \in \mathbb{N}^{n+1}$. Then the set $D_2 := \{(x_1, \ldots, x_n) \in \mathbb{N}^n : \exists z \, (z, x_1, \ldots, x_n) \in D_1\}$ is Diophantine.

So Diophantine sets are closed under conjugation ("and"), disjunction ("or"), and the existential quantifier ($\exists$).
Can also show closed under bounded universal quantifier ("for all y with $y \leq x$"), but this is a lot more work!

Diophantine sets

Theorem (Putnam, 1960)

A set $S \subset \mathbb{N}$ is Diophantine if and only if there exists a polynomial $P(x_1, \ldots, x_n)$ such that S is the nonnegative range of P (i.e. $S = \mathbb{N} \cap P(\mathbb{N}^n)$)

Diophantine sets

Theorem (Putnam, 1960)

A set $S \subset \mathbb{N}$ is Diophantine if and only if there exists a polynomial $P(x_1, \ldots, x_n)$ such that S is the nonnegative range of P (i.e. $S = \mathbb{N} \cap P(\mathbb{N}^n)$)

Proof:

- ($\Longleftarrow$) Let $S = \mathbb{N} \cap P(\mathbb{N}^n)$. Then $x \in S$ if and only if $\exists x_1, \ldots, x_n$ such that $P(x_1, \ldots, x_n) - x = 0$.

Diophantine sets

Theorem (Putnam, 1960)

A set $S \subset \mathbb{N}$ is Diophantine if and only if there exists a polynomial $P(x_1, \ldots, x_n)$ such that S is the nonnegative range of P (i.e. $S = \mathbb{N} \cap P(\mathbb{N}^n)$)

Proof:

- ($\Longleftarrow$) Let $S = \mathbb{N} \cap P(\mathbb{N}^n)$. Then $x \in S$ if and only if $\exists x_1, \ldots, x_n$ such that $P(x_1, \ldots, x_n) - x = 0$.
- ($\Longrightarrow$) Let S be Diophantine. So $x \in S$ if and only if $\exists y_1, \ldots y_m$ such that $Q(x, y_1, \ldots, y_m) = 0$.

Diophantine sets

Theorem (Putnam, 1960)

A set $S \subset \mathbb{N}$ is Diophantine if and only if there exists a polynomial $P(x_1, \ldots, x_n)$ such that S is the nonnegative range of P (i.e. $S = \mathbb{N} \cap P(\mathbb{N}^n)$)

Proof:

- ($\Longleftarrow$) Let $S = \mathbb{N} \cap P(\mathbb{N}^n)$. Then $x \in S$ if and only if $\exists x_1, \ldots, x_n$ such that $P(x_1, \ldots, x_n) - x = 0$.
- ($\Longrightarrow$) Let S be Diophantine. So $x \in S$ if and only if $\exists y_1, \ldots y_m$ such that $Q(x, y_1, \ldots, y_m) = 0$.
- Define the polynomial

$$P(x, y_1, \ldots, y_m) := (x+1)(1 - Q^2(x, y_1, \ldots, y_m)) - 1,$$

then $x \in S$ if and only if $x \in \mathbb{N} \cap P(\mathbb{N}^n)$. □

Goldbach's conjecture

Goldbach's conjecture (1742)

Every positive even integer greater than 2 is the sum of two primes.

Goldbach's conjecture

Goldbach's conjecture (1742)

Every positive even integer greater than 2 is the sum of two primes.

Note that some even integer n is a counterexample to Goldbach, if and only if, for all $z \in \{2, 3, \ldots, n-2\}$, either z is composite or $n - z$ is composite.

Goldbach's conjecture

Goldbach's conjecture (1742)

Every positive even integer greater than 2 is the sum of two primes.

Note that some even integer n is a counterexample to Goldbach, if and only if, for all $z \in \{2, 3, \ldots, n-2\}$, either z is composite or $n - z$ is composite.
Letting $n = 2a + 4$, we have Goldbach's conjecture is false if and only if

$$(\exists a)(\forall z)_{\leq a}(\exists x, y)(z + 2 - (x + 2)(y + 2))(2a + 2 - z - (x + 2)(y + 2)) = 0.$$

Goldbach's conjecture

Goldbach's conjecture (1742)

Every positive even integer greater than 2 is the sum of two primes.

Note that some even integer n is a counterexample to Goldbach, if and only if, for all $z \in \{2, 3, \ldots, n-2\}$, either z is composite or $n - z$ is composite.
Letting $n = 2a + 4$, we have Goldbach's conjecture is false if and only if

$$(\exists a)(\forall z)_{\leq a}(\exists x, y)(z + 2 - (x + 2)(y + 2))(2a + 2 - z - (x + 2)(y + 2)) = 0.$$

As applying bounded universal quantifier to a Diophantine set yields another Diophantine set (proof omitted), this yields the following theorem:

Theorem

There exists a Diophantine equation that has no solutions if and only if Goldbach's conjecture is true.

Computability

Definition

A set $S \subset \mathbb{N}^n$ is **computably enumerable** (or **listable**) if there exists an algorithm which prints out every element of S (in some order, possibly with repetitions).

Computability

Definition

A set $S \subset \mathbb{N}^n$ is **computably enumerable** (or **listable**) if there exists an algorithm which prints out every element of S (in some order, possibly with repetitions).

Theorem

Every Diophantine set is computably enumerable

Computability

Definition

A set $S \subset \mathbb{N}^n$ is **computably enumerable** (or **listable**) if there exists an algorithm which prints out every element of S (in some order, possibly with repetitions).

Theorem

Every Diophantine set is computably enumerable

Proof: Let D be a Diophantine set represented by $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$. Enumerate all $(n+m)$ tuples in some order, and for each such tuple, check whether the equality $P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$ holds or not. If it does, output $(x_1, \ldots, x_n)$. □

Computability

Definition

A set $S \subset \mathbb{N}^n$ is **computably enumerable** (or **listable**) if there exists an algorithm which prints out every element of S (in some order, possibly with repetitions).

Theorem

Every Diophantine set is computably enumerable

Proof: Let D be a Diophantine set represented by $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$. Enumerate all $(n+m)$ tuples in some order, and for each such tuple, check whether the equality $P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$ holds or not. If it does, output $(x_1, \ldots, x_n)$. □

Proving the converse is not as easy...

Turing machines

Definition (informal)

A **Turing machine** is some finite length program (e.g. some piece of code in C++).

Turing machines

Definition (informal)

A **Turing machine** is some finite length program (e.g. some piece of code in C++).

Theorem (Halting problem (Turing 1937))

There is no Turing machine which can determine if any given Turing machine halts on a given input.

Turing machines

Definition (informal)

A **Turing machine** is some finite length program (e.g. some piece of code in C++).

Theorem (Halting problem (Turing 1937))

There is no Turing machine which can determine if any given Turing machine halts on a given input.

Proof: List all Turing machines as $T_1, T_2, \ldots$. Assume there exists a Turing machine $V(n, m)$ which determines whether $T_n(m)$ halts.

Turing machines

Definition (informal)

A **Turing machine** is some finite length program (e.g. some piece of code in C++).

Theorem (Halting problem (Turing 1937))

There is no Turing machine which can determine if any given Turing machine halts on a given input.

Proof: List all Turing machines as $T_1, T_2, \ldots$. Assume there exists a Turing machine $V(n, m)$ which determines whether $T_n(m)$ halts. Construct a Turing machine $U(n)$ as follows:

- If V says $T_n(n)$ does not halt, then $U(n)$ halts.
- If V says $T_n(n)$ halts, then $U(n)$ does not halt.

Turing machines

Definition (informal)

A **Turing machine** is some finite length program (e.g. some piece of code in C++).

Theorem (Halting problem (Turing 1937))

There is no Turing machine which can determine if any given Turing machine halts on a given input.

Proof: List all Turing machines as $T_1, T_2, \ldots$. Assume there exists a Turing machine $V(n, m)$ which determines whether $T_n(m)$ halts. Construct a Turing machine $U(n)$ as follows:

- If V says $T_n(n)$ does not halt, then $U(n)$ halts.
- If V says $T_n(n)$ halts, then $U(n)$ does not halt.

For some k, $U(n) = T_k(n)$. But then $U(k)$ halts iff $T_k(k)$ halts, contradiction. □

Decidable set

Definition

A set $S \subset \mathbb{N}^n$ is **decidable** if both S and its complement are computably enumerable. Equivalently, given any $\underline{n} \in \mathbb{N}^n$ there exists an algorithm to determine whether $\underline{n} \in S$.

Decidable set

Definition

A set $S \subset \mathbb{N}^n$ is **decidable** if both S and its complement are computably enumerable. Equivalently, given any $\underline{n} \in \mathbb{N}^n$ there exists an algorithm to determine whether $\underline{n} \in S$.

Obviously, every decidable set is computably enumerable. What about the converse?

Decidable set

Definition

A set $S \subset \mathbb{N}^n$ is **decidable** if both S and its complement are computably enumerable. Equivalently, given any $\underline{n} \in \mathbb{N}^n$ there exists an algorithm to determine whether $\underline{n} \in S$.

Obviously, every decidable set is computably enumerable. What about the converse?

Theorem

There exists a set U which is computably enumerable but no decidable.

Decidable set

Definition

A set $S \subset \mathbb{N}^n$ is **decidable** if both S and its complement are computably enumerable. Equivalently, given any $\underline{n} \in \mathbb{N}^n$ there exists an algorithm to determine whether $\underline{n} \in S$.

Obviously, every decidable set is computably enumerable. What about the converse?

Theorem

There exists a set U which is computably enumerable but no decidable.

Proof: Enumerate all Turing machines as $T_1, T_2, \ldots$. Construct a computably enumerable set $S \subset \mathbb{N} \times \mathbb{N}$ as follows:

Decidable set

Definition

A set $S \subset \mathbb{N}^n$ is **decidable** if both S and its complement are computably enumerable. Equivalently, given any $\underline{n} \in \mathbb{N}^n$ there exists an algorithm to determine whether $\underline{n} \in S$.

Obviously, every decidable set is computably enumerable. What about the converse?

Theorem

There exists a set U which is computably enumerable but no decidable.

Proof: Enumerate all Turing machines as $T_1, T_2, \ldots$. Construct a computably enumerable set $S \subset \mathbb{N} \times \mathbb{N}$ as follows:

1: **for all** $(m, n, x) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ **do**
2: Run $T_n(m)$ for exactly x steps. If this halts, then add (m, n) to S.

Decidable set

Definition

A set $S \subset \mathbb{N}^n$ is **decidable** if both S and its complement are computably enumerable. Equivalently, given any $\underline{n} \in \mathbb{N}^n$ there exists an algorithm to determine whether $\underline{n} \in S$.

Obviously, every decidable set is computably enumerable. What about the converse?

Theorem

There exists a set U which is computably enumerable but no decidable.

Proof: Enumerate all Turing machines as $T_1, T_2, \ldots$. Construct a computably enumerable set $S \subset \mathbb{N} \times \mathbb{N}$ as follows:

1: **for all** $(m, n, x) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ **do**
2: Run $T_n(m)$ for exactly x steps. If this halts, then add (m, n) to S.

If S were decidable, then there exists algorithm which determines if $T_n(m)$ halts, contradiction. □

Main theorem

Theorem (Matiyasevich–Robinson–Davis–Putnam, 1970)

Every computably enumerable set is Diophantine.

Main theorem

Theorem (Matiyasevich–Robinson–Davis–Putnam, 1970)

Every computably enumerable set is Diophantine.

A full proof is rather long, but each step is relatively elementary.

Main theorem

Theorem (Matiyasevich–Robinson–Davis–Putnam, 1970)

Every computably enumerable set is Diophantine.

A full proof is rather long, but each step is relatively elementary.

- Martin Davis showed that, for any computably enumerable set S, there exists a polynomial $P(x, y, k, z_1, \ldots, z_n)$ such that

$$x \in S \iff \exists y \forall k \leq y, \exists z_1, \ldots, z_n \leq y : P(x, y, k, z_1, \ldots, z_n) = 0$$

(see Davis's *Computability and Unsolvability*)

Main theorem

Theorem (Matiyasevich–Robinson–Davis–Putnam, 1970)

Every computably enumerable set is Diophantine.

A full proof is rather long, but each step is relatively elementary.

- Martin Davis showed that, for any computably enumerable set S, there exists a polynomial $P(x, y, k, z_1, \ldots, z_n)$ such that

$$x \in S \iff \exists y \forall k \leq y, \exists z_1, \ldots, z_n \leq y : P(x, y, k, z_1, \ldots, z_n) = 0$$

  (see Davis's *Computability and Unsolvability*)

- Davis conjectures in the early 1950s that every computably enumerable set is Diophantine.

Main theorem

- In 1961, Martin Davis, Hilary Putnam and Julia Robinson prove, that for any computably enumerable set S, there exists an **exponential Diophantine equation** $E(x, y_1, \ldots, y_m)$ such that

$$x \in S \iff \exists y_1, \ldots, y_m : E(x, y_1, \ldots, y_m) = 0.$$

  Here, E is built from $x, y_1, \ldots, y_m$ and $\mathbb{N}$ by addition, subtraction, multiplication and exponentiation. (e.g. $2x^y + y^{z+x}$ is exponential Diophantine)

Main theorem

- In 1961, Martin Davis, Hilary Putnam and Julia Robinson prove, that for any computably enumerable set S, there exists an **exponential Diophantine equation** $E(x, y_1, \ldots, y_m)$ such that

$$x \in S \iff \exists y_1, \ldots, y_m : E(x, y_1, \ldots, y_m) = 0.$$

  Here, E is built from $x, y_1, \ldots, y_m$ and $\mathbb{N}$ by addition, subtraction, multiplication and exponentiation. (e.g. $2x^y + y^{z+x}$ is exponential Diophantine)

- In 1970, Yuri Matiyasevich showed that the set

$$\{(x, y) \in \mathbb{N}^2 : y = F_{2x}\}$$

  is Diophantine. Combining this with earlier work by Davis–Putnam–Robinson, this proves that every computably enumerable set is Diophantine. □

Hilbert's 10th problem

Theorem (Negative solution to Hilbert's 10th problem)

There does not exist an algorithm to determine if an arbitrary Diophantine equation $P(x_1, \ldots, x_n) = 0$ *has natural solutions.*

Hilbert's 10th problem

Theorem (Negative solution to Hilbert's 10th problem)

There does not exist an algorithm to determine if an arbitrary Diophantine equation $P(x_1, \ldots, x_n) = 0$ *has natural solutions.*

Proof:

- Suppose such an algorithm exists. Let $U \subset \mathbb{N}$ be a computably enumerable but not decidable set.

Hilbert's 10th problem

Theorem (Negative solution to Hilbert's 10th problem)

There does not exist an algorithm to determine if an arbitrary Diophantine equation $P(x_1, \ldots, x_n) = 0$ has natural solutions.

Proof:

- Suppose such an algorithm exists. Let $U \subset \mathbb{N}$ be a computably enumerable but not decidable set.
- By the MRDP theorem, U is Diophantine, and thus there exists polynomial P such that $P(x, y_1, \ldots, y_m) = 0$ if and only if $x \in U$.

Hilbert's 10th problem

Theorem (Negative solution to Hilbert's 10th problem)

There does not exist an algorithm to determine if an arbitrary Diophantine equation $P(x_1, \ldots, x_n) = 0$ has natural solutions.

Proof:

- Suppose such an algorithm exists. Let $U \subset \mathbb{N}$ be a computably enumerable but not decidable set.
- By the MRDP theorem, U is Diophantine, and thus there exists polynomial P such that $P(x, y_1, \ldots, y_m) = 0$ if and only if $x \in U$.
- But our algorithm would then allow us to decide whether $x \in U$ for any $x \in \mathbb{N}$, contradicting U not decidable. □

Rational solutions

Question

Does there exist algorithm whether any given polynomial equation $p(x_1, \ldots, x_n) = 0$ has rational solution $x_1, \ldots, x_n \in \mathbb{Q}$?

Rational solutions

Question

Does there exist algorithm whether any given polynomial equation $p(x_1, \ldots, x_n) = 0$ has rational solution $x_1, \ldots, x_n \in \mathbb{Q}$?

A polynomial $P(x_1, \ldots, x_n)$ has a solution over the rationals if and only if

$$(z+1)^d P\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_n - y_n}{z+1}\right) = 0$$

has a solution over $\mathbb{N}$.

Rational solutions

Question

Does there exist algorithm whether any given polynomial equation $p(x_1, \ldots, x_n) = 0$ has rational solution $x_1, \ldots, x_n \in \mathbb{Q}$?

A polynomial $P(x_1, \ldots, x_n)$ has a solution over the rationals if and only if

$$(z+1)^d P\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_n - y_n}{z+1}\right) = 0$$

has a solution over $\mathbb{N}$.

A positive answer to H10 over $\mathbb{Z}$ would've implied a positive answer to H10 over the rationals! But a negative answer to H10 doesn't tell us anything about H10 over $\mathbb{Q}$, unless $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$. (*it's probably not?*)
(i.e. does there exist P such that $\mathbb{Z} = \{x \in \mathbb{Q} : \exists y_1, \ldots, y_m \in \mathbb{Q}, P(x, y_1, \ldots, y_m) = 0\}$?)

Prime numbers

Theorem

There exists a polynomial P such that $P(x_1, \ldots, x_n) = a$ has a solution if and only if a is prime.

Prime numbers

Theorem

There exists a polynomial P such that $P(x_1, \ldots, x_n) = a$ has a solution if and only if a is prime.

One can explicitly construct such a polynomial!

Prime numbers

Theorem

There exists a polynomial P such that $P(x_1, \ldots, x_n) = a$ has a solution if and only if a is prime.

One can explicitly construct such a polynomial!

1. Show the powers of 2 $\{2^n\}$ is Diophantine.

Prime numbers

Theorem

There exists a polynomial P such that $P(x_1, \ldots, x_n) = a$ has a solution if and only if a is prime.

One can explicitly construct such a polynomial!

1. Show the powers of 2 $\{2^n\}$ is Diophantine.
2. Show the binomial coefficients $\{c = \binom{a}{b}\}$ is Diophantine.

Prime numbers

Theorem

There exists a polynomial P such that $P(x_1, \ldots, x_n) = a$ has a solution if and only if a is prime.

One can explicitly construct such a polynomial!

1. Show the powers of 2 $\{2^n\}$ is Diophantine.
2. Show the binomial coefficients $\{c = \binom{a}{b}\}$ is Diophantine.
3. Show factorials $\{n!\}$ is Diophantine.

Prime numbers

Theorem

There exists a polynomial P such that $P(x_1, \ldots, x_n) = a$ has a solution if and only if a is prime.

One can explicitly construct such a polynomial!

1. Show the powers of 2 $\{2^n\}$ is Diophantine.
2. Show the binomial coefficients $\{c = \binom{a}{b}\}$ is Diophantine.
3. Show factorials $\{n!\}$ is Diophantine.
4. Use Wilson's theorem: $(n-1)! \equiv -1 \pmod{n}$ if and only if n prime.

Prime numbers

Theorem (Jones–Sato–Wada–Wiens, 1975)

The set of prime numbers is identical to the set of positive values taken on by the polynomial

$$
\begin{aligned}
&(k+2)(1-(wz+h+j-q)^2-((gk+2g+k+1)(h+j)+h-z)^2\\
&\quad-(2n+p+q+z-e)^2-(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2\\
&\quad-(e^3(e+2)(a+1)^2+1-o^2)^2-((a^2-1)y^2+1-x^2)^2\\
&\quad-(16r^2y^4(a^2-1)+1-u^2)^2-(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2)^2\\
&\quad-(n+l+v-y)^2-((a^2-1)l^2+1-m^2)^2-(ai+k+1-l-i)^2\\
&\quad-(p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m)^2\\
&\quad-(q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x)^2\\
&\quad-(z+pl(a-p)+t(2ap-p^2-1)-pm)^2
\end{aligned}
$$

as the variables $a, b, \ldots, z$ range over the nonnegative integers.

Universality theorem

As integer polynomials countably infinite, we can enumerate all Diophantine sets $D_1, D_2, \ldots$.

Theorem (Universality theorem)

The set $\{(n, x) : x \in D_n\}$ is Diophantine.

Universality theorem

As integer polynomials countably infinite, we can enumerate all Diophantine sets $D_1, D_2, \ldots$.

Theorem (Universality theorem)

The set $\{(n, x) : x \in D_n\}$ is Diophantine.

Proof:

- As Diophantine sets are computably enumerably, for each $n \in \mathbb{N}$, there exists a Turing machine T_n which outputs the set D_n.

Universality theorem

As integer polynomials countably infinite, we can enumerate all Diophantine sets $D_1, D_2, \ldots$.

Theorem (Universality theorem)

The set $\{(n, x) : x \in D_n\}$ is Diophantine.

Proof:

- As Diophantine sets are computably enumerably, for each $n \in \mathbb{N}$, there exists a Turing machine T_n which outputs the set D_n.
- Now run the following algorithm:

1: **for all** $(n, m, x) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ **do**
2: Run T_n for exactly m steps. If this outputs x, then output (n, x)

Universality theorem

As integer polynomials countably infinite, we can enumerate all Diophantine sets $D_1, D_2, \ldots$.

Theorem (Universality theorem)

The set $\{(n, x) : x \in D_n\}$ is Diophantine.

Proof:

- As Diophantine sets are computably enumerably, for each $n \in \mathbb{N}$, there exists a Turing machine T_n which outputs the set D_n.
- Now run the following algorithm:

  1: **for all** $(n, m, x) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ **do**
  2: Run T_n for exactly m steps. If this outputs x, then output (n, x)

- Thus $\{(n, x) : x \in D_n\}$ is computably enumerable, and so by MRDP is Diophantine.

□

Universal Diophantine system

Theorem (Jones, 1982)

There exists an enumeration of Diophantine sets $D_1, D_2, \ldots$, such that $x \in D_v$ if and only if the equation

$$
\begin{aligned}
&(elg^2 + \alpha - (b - xy)q^2)^2 + (q - b^{5^{60}})^2 + (\lambda + q^4 - 1 - \lambda b^5)^2 + (\theta + 2z - b^5)^2 \\
&\quad + (u + t\theta - l)^2 + (y + m\theta - e)^2 + (n - q^{16})^2 + ((g + eq^3 + lq^5 \\
&\quad + (2(e - z\lambda)(1 + xb^5 + g)^4 + \lambda b^5 + \lambda b^5 q^4)q^4)(n^2 - n) + (q^3 - bl + l + \theta\lambda q^3 \\
&\quad + (b^5 - 2)q^5)(n^2 - 1) - r)^2 + (p - 2ws^2 r^2 n^2)^2 + (p^2 k^2 - k^2 + 1 - \tau^2)^2 \\
&\quad + (4(c - ksn^2)^2 + \eta - k^2)^2 + (r + 1 + hp - h - k)^2 + (a - (wn^2 + 1)rsn^2)^2 \\
&\quad + (2r + 1 + \phi - c)^2 + (bw + ca - 2c + 4\alpha\gamma - 5\gamma - d)^2 + ((a^2 - 1)c^2 + 1 - d^2)^2 \\
&\quad + ((a^2 - 1)i^2 c^4 + 1 - f^2)^2 + (((a + f^2(d^2 - a))^2 - 1)(2r + 1 + jc)^2 \\
&\quad + 1 - (d + of)^2)^2 + (((z + u + y)^2 + u)^2 + y - v)^2 = 0
\end{aligned}
$$

has a solution.

Bounds on P

By replacing high degree equations of others with low degree (e.g. set $z_i = x_j x_k$ and $z_i = x_j^2$), the degree of the entire system can be brought down to 2. Then summing the squares yields an equation of degree 4.

Bounds on P

By replacing high degree equations of others with low degree (e.g. set $z_i = x_j x_k$ and $z_i = x_j^2$), the degree of the entire system can be brought down to 2. Then summing the squares yields an equation of degree 4.

Applying this procedure to the above polynomial gives a degree 4 equation in 58 unknowns.

Bounds on P

By replacing high degree equations of others with low degree (e.g. set $z_i = x_j x_k$ and $z_i = x_j^2$), the degree of the entire system can be brought down to 2. Then summing the squares yields an equation of degree 4.

Applying this procedure to the above polynomial gives a degree 4 equation in 58 unknowns.

Theorem (Jones, 1982)

Every Diophantine equation is equivalent to solving another Diophantine equation of degree d in m unknowns where (d, m) is any one of the following pairs:

$$(4, 58), (8, 38), (12, 32), (16, 29), (20, 28), (24, 26), (28, 25), (36, 24),$$
$$(96, 21), (2668, 19), (2 \times 10^5, 14), (6.6 \times 10^{43}, 13), (1.3 \times 10^{44}, 12),$$
$$(4.6 \times 10^{44}, 11), (8.6 \times 10^{24}, 10), (1.6 \times 10^{45}, 9)$$

Time complexity

For which Diophantine equations does an algorithm exist?

Time complexity

For which Diophantine equations does an algorithm exist?

Theorem (Siegel (1972))

There exists an algorithm to determine whether any degree two polynomial equation $p(x_1, \ldots, x_n) = 0$ *has integer solutions.*

Time complexity

For which Diophantine equations does an algorithm exist?

Theorem (Siegel (1972))

There exists an algorithm to determine whether any degree two polynomial equation $p(x_1, \ldots, x_n) = 0$ *has integer solutions.*

For which Diophantine equations does a practical algorithm exist?

Time complexity

For which Diophantine equations does an algorithm exist?

Theorem (Siegel (1972))

There exists an algorithm to determine whether any degree two polynomial equation $p(x_1, \ldots, x_n) = 0$ *has integer solutions.*

For which Diophantine equations does a practical algorithm exist?

Theorem (Adleman, Manders (1976))

The problem: "Given $a, b, c \in \mathbb{N}$*, does there exist* $x, y \in \mathbb{Z}$ *such that* $ax^2 + by + c = 0$*?" is NP-complete.*

Time complexity

For which Diophantine equations does an algorithm exist?

Theorem (Siegel (1972))

There exists an algorithm to determine whether any degree two polynomial equation $p(x_1, \ldots, x_n) = 0$ has integer solutions.

For which Diophantine equations does a practical algorithm exist?

Theorem (Adleman, Manders (1976))

The problem: "Given $a, b, c \in \mathbb{N}$, does there exist $x, y \in \mathbb{Z}$ such that $ax^2 + by + c = 0$?" is NP-complete.

i.e. If you can find an algorithm which solves the above problem in at most $\mathcal{O}((\log a + \log b + \log c)^k)$ steps for some k, then you'll have shown P=NP and win \$1 000 000!

Further Applications

Theorem

There exists a Diophantine equation that has no solutions if and only if ZFC is consistent.

Further Applications

Theorem

There exists a Diophantine equation that has no solutions if and only if ZFC is consistent.

Proof: List all theorems in some order $T_1, T_2, \ldots$. Let $\mathrm{Prop}(n)$ be the statement "there is no contradiction among the first n theorems". As $\mathrm{Prop}(n)$ is decidable, there exists a Diophantine equation with no solutions if and only if $\mathrm{Prop}(n)$ holds for all n.

Further Applications

Theorem

There exists a Diophantine equation that has no solutions if and only if ZFC is consistent.

Proof: List all theorems in some order $T_1, T_2, \ldots$. Let $\mathrm{Prop}(n)$ be the statement "there is no contradiction among the first n theorems". As $\mathrm{Prop}(n)$ is decidable, there exists a Diophantine equation with no solutions if and only if $\mathrm{Prop}(n)$ holds for all n.

Theorem

There exists a Diophantine equation that has no solutions if and only if Peano arithmetic is consistent.

Further Applications

Theorem

There exists a Diophantine equation that has no solutions if and only if ZFC is consistent.

Proof: List all theorems in some order $T_1, T_2, \ldots$. Let $\mathrm{Prop}(n)$ be the statement "there is no contradiction among the first n theorems". As $\mathrm{Prop}(n)$ is decidable, there exists a Diophantine equation with no solutions if and only if $\mathrm{Prop}(n)$ holds for all n.

Theorem

There exists a Diophantine equation that has no solutions if and only if Peano arithmetic is consistent.

Theorem

There exists a Diophantine equation that has no solutions if and only if ZFC$^+$ is consistent.

Extensions

Is Hilbert's Tenth Problem solvable over more general rings?

Extensions

Is Hilbert's Tenth Problem solvable over more general rings?

Definition

Let $\mathcal{O}_K$ be the ring of integers of some number field K. A set $S \subset \mathcal{O}_K^n$ is **Diophantine in** $\mathcal{O}_K$ if there exists a polynomial $f \in \mathcal{O}_K[x_1, \ldots, x_n, y_1 \ldots, y_m]$ such that

$$(a_1, \ldots, a_n) \in S \iff \exists b_1, \ldots, b_m : f(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0.$$

Extensions

Is Hilbert's Tenth Problem solvable over more general rings?

Definition

Let $\mathcal{O}_K$ be the ring of integers of some number field K. A set $S \subset \mathcal{O}_K^n$ is **Diophantine in** $\mathcal{O}_K$ if there exists a polynomial $f \in \mathcal{O}_K[x_1, \ldots, x_n, y_1 \ldots, y_m]$ such that

$$(a_1, \ldots, a_n) \in S \iff \exists b_1, \ldots, b_m : f(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0.$$

Theorem

Let K be number field. If $\mathbb{Z}$ is Diophantine in $\mathcal{O}_K$, then Hilbert 10 is unsolvable over $\mathcal{O}_K$.

Extensions

Is Hilbert's Tenth Problem solvable over more general rings?

Definition

Let $\mathcal{O}_K$ be the ring of integers of some number field K. A set $S \subset \mathcal{O}_K^n$ is **Diophantine in** $\mathcal{O}_K$ if there exists a polynomial $f \in \mathcal{O}_K[x_1, \ldots, x_n, y_1 \ldots, y_m]$ such that

$$(a_1, \ldots, a_n) \in S \iff \exists b_1, \ldots, b_m : f(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0.$$

Theorem

Let K be number field. If $\mathbb{Z}$ is Diophantine in $\mathcal{O}_K$, then Hilbert 10 is unsolvable over $\mathcal{O}_K$.

Proof: Let f represent $\mathbb{Z}$ Diophantine in $\mathcal{O}_K$. Then for any polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots x_n]$, this has a solution over $\mathbb{Z}$ if and only if the system

$$p(x_1, \ldots, x_n) = 0. \quad f(x_1, y_{1,1}, \ldots, y_{1,m}) = 0, \quad , \ldots, \quad f(x_n, y_{n,1}, \ldots, y_{n,m}) = 0$$

has a solution over $\mathcal{O}_K$. So if Hilbert 10 were solvable over $\mathcal{O}_K$, this would contradict the unsolvability of Hilbert 10 over $\mathbb{Z}$. □

Extensions

Theorem (Denef (1980), Pheidas (1988), Shlapentokh (1989))

Let K be a number field satisfying any one of the following three cases:

1. *K is totally real, or quadratic extension of totally real field.*
2. *K has exactly one non-real archimedean place.*
3. *K is subfield of any of the above cases.*

Then Hilbert's 10th problem is unsolvable over $\mathcal{O}_K$.

Extensions

Theorem (Denef (1980), Pheidas (1988), Shlapentokh (1989))

Let K be a number field satisfying any one of the following three cases:

1. *K is totally real, or quadratic extension of totally real field.*
2. *K has exactly one non-real archimedean place.*
3. *K is subfield of any of the above cases.*

Then Hilbert's 10th problem is unsolvable over $\mathcal{O}_K$.

Corollary (Shapiro, Shlapentokh (1989))

Let K be a number field such that $Gal(K/\mathbb{Q})$ is abelian. Then Hilbert's 10th problem is unsolvable for $\mathcal{O}_K$.

Summary

Table: Summary of answers to Hilbert's tenth problem over various rings R (Poonen 2003).

Ring R	Hilbert 10	Authors
$\mathbb{C}$	**Yes**	(elimination theory)
$\mathbb{R}$	**Yes**	Tarski (1951)
$\mathbb{F}_q$	**Yes**	(trivial)
p-adic fields	**Yes**	Nerode (1963)
number field	?	
$\mathbb{Q}$	?	
global function field	**No**	Shlapentokh (1992), Eisenträger (2003)
$\mathbb{F}_q(t)$	**No**	Pheidas (1991), Videla (1994)
$\mathcal{O}_K$	? (No for some $\mathcal{O}_K$)	
$\mathbb{Z}$	**No**	MRDP (1970)

Elliptic curves

Can we use elliptic curves E/K to cut out integral Diophantine sets over an extension of numbers fields?

Elliptic curves

Can we use elliptic curves E/K to cut out integral Diophantine sets over an extension of numbers fields?

Theorem (Poonen, 2002)

Let L/K be finite extension of number fields. Suppose there exists an elliptic curve E/K sch that

$$rank\ E(L) = rank\ E(K) = 1$$

Then $\mathcal{O}_K$ is Diophantine in $\mathcal{O}_L$.

Elliptic curves

Can we use elliptic curves E/K to cut out integral Diophantine sets over an extension of numbers fields?

Theorem (Poonen, 2002)

Let L/K be finite extension of number fields. Suppose there exists an elliptic curve E/K sch that

$$rank\ E(L) = rank\ E(K) = 1$$

Then $\mathcal{O}_K$ is Diophantine in $\mathcal{O}_L$.

Conjecture (Poonen, 2002)

For every number field K, there exists an elliptic curve $E/\mathbb{Q}$ such that $\text{rank}E(\mathbb{Q}) = \text{rank}E(K) = 1$.

Elliptic curves

Theorem (Cornelissen, Pheidas, Zahidi (2005), Shlapentokh (2008))

Let L/K be finite extension of number fields. Suppose there exists an elliptic curve E/K sch that

$$rank\ E(L) = rank\ E(K) > 0$$

Then $\mathcal{O}_K$ is Diophantine in $\mathcal{O}_L$.

Elliptic curves

Theorem (Cornelissen, Pheidas, Zahidi (2005), Shlapentokh (2008))

Let L/K be finite extension of number fields. Suppose there exists an elliptic curve E/K sch that

$$rank\ E(L) = rank\ E(K) > 0$$

Then $\mathcal{O}_K$ is Diophantine in $\mathcal{O}_L$.

Theorem (Mazur, Rubin, Shlapentokh (2022))

Let K be a number field and L an algebraic extension of K. Suppose there exists an abelian variety A/K such that $rankA(L) = rankA(K) > 0$. If L satisfies either one of the following two conditions:

1. *L is a number field.*
2. *L is totally real, or quadratic extension of totally real field.*

Then $\mathcal{O}_K$ is Diophantine in $\mathcal{O}_L$.

Elliptic curves

Theorem (Mazur, Rubin (2010))

If $Ш(E/K)[2]$ is a perfect square for every elliptic curve E/K, for any number field K, then H10 is unsolvable for all $\mathcal{O}_K$.

Elliptic curves

Theorem (Mazur, Rubin (2010))

If $Ш(E/K)[2]$ is a perfect square for every elliptic curve E/K, for any number field K, then H10 is unsolvable for all $\mathcal{O}_K$.

Theorem (Murty, Pasten (2018))

Assume that elliptic curves are automorphic, satisfy the parity conjecture, and that for every Grössencharacter ψ,

$$ord_{s=1} L(E/K, s, \psi) = 0 \implies dim(E(L) \otimes \mathbb{C})^{\psi} = 0.$$

Then H10 is unsolvable for every $\mathcal{O}_K$.

References


Davis, M. (1958)
Computability and unsolvability.
McGraw-Hill Book Co., Inc., New York-Toronto-London.


Davis, M., Putnam, H., Robinson, J. (1961)
The decision problem for exponential diophantine equations.
Ann. of Math. (2) 74, 425–436.


Davis, M. (1973)
Hilbert's tenth problem is unsolvable.
Amer. Math. Monthly 80, 233–269.


Jones, J.P., Sato, D., Wada, H., Wiens, D. (1976)
Diophantine representation of the set of prime numbers.
Amer. Math. Monthly 83, no. 6, 449–464.

References


Jones, J.P. (1982)
Universal Diophantine Equation
J. Symbolic Logic 47, no. 3, 549–571.


Manders, K.L., Adleman, L. (1978)
NP-complete decision problems for binary quadratics.
Journal of Computer and System Sciences, 16(2), pp.168-184.


Matijasevič, Ju. V. (1970)
The Diophantineness of enumerable sets. (Russian)
Dokl. Akad. Nauk SSSR 191 279–282.


Murty, M.R., Fodden, B. (2019)
Hilbert's Tenth Problem: An Introduction to Logic, Number Theory, and Computability
American Mathematical Society, Providence, Rhode Island.

References

Poonen, B. (2002)

Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers

In: *Algorithmic number theory (Sydney, 2002)*, 33-42. Springer, Berlin, Heidelberg.

Poonen, B. (2003)

Hilbert's Tenth Problem over rings of number-theoretic interest.

Arizona Winter School, Number theory and logic.

Putnam, H. (1960)

An unsolvable problem in number theory.

J. Symbolic Logic 25, 220–232.

Turing, A.M. (1938)

On computable numbers, with an application to the Entscheidungsproblem. A correction.

Proceedings of the London Mathematical Society, 2(1), pp.544-546.

Questions?