Undecidability of Hilbert's Tenth Problem and its Applications

Takao Yuyama

Automata and Logic Workshop in AKITA
March 27, 2019

Tokyo Institute of Technology

Table of Contents

Table of Contents

Diophantine Equations

Solving Diophantine equations is one of the most important problem in number theory.

For example, Fermat's last theorem says that none of the infinitely many Diophantine equations

$$x^3 + y^3 = z^3, x^4 + y^4 = z^4, x^5 + y^5 = z^5, \dots$$

have nontrivial solution in $\mathbb{Z}$.

Here are other examples.

$x^3 + y^3 + z^3 = 29$
$x^3 + y^3 + z^3 = 30$
$x^3 + y^3 + z^3 = 31$
$x^3 + y^3 + z^3 = 32$
$x^3 + y^3 + z^3 = 33$

Diophantine Equations

Solving Diophantine equations is one of the most important problem in number theory.

For example, Fermat's last theorem says that none of the infinitely many Diophantine equations

$$x^3 + y^3 = z^3, x^4 + y^4 = z^4, x^5 + y^5 = z^5, \dots$$

have nontrivial solution in $\mathbb{Z}$.

Here are other examples.

$x^3 + y^3 + z^3 = 29$

$x^3 + y^3 + z^3 = 30$

$x^3 + y^3 + z^3 = 31$

$x^3 + y^3 + z^3 = 32$

$x^3 + y^3 + z^3 = 33$

Diophantine Equations

Solving Diophantine equations is one of the most important problem in number theory.

For example, Fermat's last theorem says that none of the infinitely many Diophantine equations

$$x^3 + y^3 = z^3, x^4 + y^4 = z^4, x^5 + y^5 = z^5, \dots$$

have nontrivial solution in $\mathbb{Z}$.

Here are other examples.

$x^3 + y^3 + z^3 = 29$
$x^3 + y^3 + z^3 = 30$
$x^3 + y^3 + z^3 = 31$
$x^3 + y^3 + z^3 = 32$
$x^3 + y^3 + z^3 = 33$

Diophantine Equations

Solving Diophantine equations is one of the most important problem in number theory.

For example, Fermat's last theorem says that none of the infinitely many Diophantine equations

$$x^3 + y^3 = z^3, x^4 + y^4 = z^4, x^5 + y^5 = z^5, \dots$$

have nontrivial solution in $\mathbb{Z}$.

Here are other examples.

$x^3 + y^3 + z^3 = 29 \quad (x, y, z) = (3, 1, 1)$

$x^3 + y^3 + z^3 = 30$

$x^3 + y^3 + z^3 = 31$

$x^3 + y^3 + z^3 = 32$

$x^3 + y^3 + z^3 = 33$

Diophantine Equations

Solving Diophantine equations is one of the most important problem in number theory.

For example, Fermat's last theorem says that none of the infinitely many Diophantine equations

$$x^3 + y^3 = z^3, x^4 + y^4 = z^4, x^5 + y^5 = z^5, \dots$$

have nontrivial solution in $\mathbb{Z}$.

Here are other examples.

$x^3 + y^3 + z^3 = 29 \quad (x, y, z) = (3, 1, 1)$
$x^3 + y^3 + z^3 = 30 \quad (x, y, z) = (-283059965, -2218888517, 2220422932)$
$x^3 + y^3 + z^3 = 31$
$x^3 + y^3 + z^3 = 32$
$x^3 + y^3 + z^3 = 33$

Diophantine Equations

Solving Diophantine equations is one of the most important problem in number theory.

For example, Fermat's last theorem says that none of the infinitely many Diophantine equations

$$x^3 + y^3 = z^3, x^4 + y^4 = z^4, x^5 + y^5 = z^5, \dots$$

have nontrivial solution in $\mathbb{Z}$.

Here are other examples.

$x^3 + y^3 + z^3 = 29$ $(x, y, z) = (3, 1, 1)$

$x^3 + y^3 + z^3 = 30$ $(x, y, z) = (-283059965, -2218888517, 2220422932)$

$x^3 + y^3 + z^3 = 31$ No solution (Consider $\mod 9$)

$x^3 + y^3 + z^3 = 32$

$x^3 + y^3 + z^3 = 33$

Diophantine Equations

Solving Diophantine equations is one of the most important problem in number theory.

For example, Fermat's last theorem says that none of the infinitely many Diophantine equations

$$x^3 + y^3 = z^3, x^4 + y^4 = z^4, x^5 + y^5 = z^5, \dots$$

have nontrivial solution in $\mathbb{Z}$.

Here are other examples.

$x^3 + y^3 + z^3 = 29$ $(x, y, z) = (3, 1, 1)$

$x^3 + y^3 + z^3 = 30$ $(x, y, z) = (-283059965, -2218888517, 2220422932)$

$x^3 + y^3 + z^3 = 31$ No solution (Consider $\mod 9$)

$x^3 + y^3 + z^3 = 32$ No solution (Consider $\mod 9$)

$x^3 + y^3 + z^3 = 33$

Diophantine Equations

Solving Diophantine equations is one of the most important problem in number theory.

For example, Fermat's last theorem says that none of the infinitely many Diophantine equations

$$x^3 + y^3 = z^3, x^4 + y^4 = z^4, x^5 + y^5 = z^5, \dots$$

have nontrivial solution in $\mathbb{Z}$.

Here are other examples.

$x^3 + y^3 + z^3 = 29$	$(x, y, z) = (3, 1, 1)$
$x^3 + y^3 + z^3 = 30$	$(x, y, z) = (-283059965, -2218888517, 2220422932)$
$x^3 + y^3 + z^3 = 31$	No solution (Consider $\mod 9$)
$x^3 + y^3 + z^3 = 32$	No solution (Consider $\mod 9$)
$x^3 + y^3 + z^3 = 33$	$(8866128975287528, -8778405442862239, -2736111468807040)$ (Found in March 2019)

Hilbert's Tenth Problem

Hilbert's tenth problem is the following decision problem.

Problem (Hilbert's Tenth Problem; HTP)

Input: *A (multivariate) polynomial* $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$

Question: *Is* $\exists (x_1, \ldots, x_n) \in \mathbb{Z}^n [f(x_1, \ldots, x_n) = 0]$*?*

In 1970, Y. V. Matiyasevich completed the undecidability proof of the tenth problem.

Theorem

HTP is undecidable.

Hilbert's Tenth Problem

Hilbert's tenth problem is the following decision problem.

Problem (Hilbert's Tenth Problem; HTP)

Input: *A (multivariate) polynomial* $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$

Question: *Is* $\exists (x_1, \ldots, x_n) \in \mathbb{Z}^n [f(x_1, \ldots, x_n) = 0]$*?*

In 1970, Y. V. Matiyasevich completed the undecidability proof of the tenth problem.

Theorem

HTP is undecidable.

Table of Contents

Four-Square Theorem

In order to prove the undecidability of HTP, it suffices to show that the following variant of HTP is undecidable.

Problem (HTP for $\mathbb{N}$)

Input: *A (multivariate) polynomial* $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$

Question: *Is* $\exists (x_1, \ldots, x_n) \in \mathbb{N}^n [f(x_1, \ldots, x_n) = 0]$*?*

Proof.

Thanks to Lagrange's four-square theorem, we have

$$\exists (x_1, \ldots, x_n) \in \mathbb{N}^n [f(x_1, \ldots, x_n) = 0]$$

$$\iff \left[\begin{array}{l} \exists (x_{11}, \ldots, x_{n4}) \in \mathbb{Z}^{4n} \\ \quad [f(x_{11}^2 + x_{12}^2 + x_{13}^2 + x_{14}^2, \ldots, x_{n1}^2 + x_{n2}^2 + x_{n3}^2 + x_{n4}^2) = 0] \end{array} \right]$$

for all $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$. □

Note: Undecidability status of HTP for $\mathbb{Q}$ is still open!

Four-Square Theorem

In order to prove the undecidability of HTP, it suffices to show that the following variant of HTP is undecidable.

Problem (HTP for $\mathbb{N}$)

Input: *A (multivariate) polynomial* $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$

Question: *Is* $\exists (x_1, \ldots, x_n) \in \mathbb{N}^n [f(x_1, \ldots, x_n) = 0]$*?*

Proof.

Thanks to Lagrange's four-square theorem, we have

$$\exists (x_1, \ldots, x_n) \in \mathbb{N}^n [f(x_1, \ldots, x_n) = 0]$$

$$\iff \left[\begin{array}{l} \exists (x_{11}, \ldots, x_{n4}) \in \mathbb{Z}^{4n} \\ \quad [f(x_{11}^2 + x_{12}^2 + x_{13}^2 + x_{14}^2, \ldots, x_{n1}^2 + x_{n2}^2 + x_{n3}^2 + x_{n4}^2) = 0] \end{array} \right]$$

for all $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$. □

Note: Undecidability status of HTP for $\mathbb{Q}$ is still open!

Four-Square Theorem

In order to prove the undecidability of HTP, it suffices to show that the following variant of HTP is undecidable.

Problem (HTP for $\mathbb{N}$)

Input: *A (multivariate) polynomial* $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$

Question: *Is* $\exists (x_1, \ldots, x_n) \in \mathbb{N}^n [f(x_1, \ldots, x_n) = 0]$*?*

Proof.

Thanks to Lagrange's four-square theorem, we have

$$\exists (x_1, \ldots, x_n) \in \mathbb{N}^n [f(x_1, \ldots, x_n) = 0]$$

$$\iff \left[\begin{array}{l} \exists (x_{11}, \ldots, x_{n4}) \in \mathbb{Z}^{4n} \\ \quad [f(x_{11}^2 + x_{12}^2 + x_{13}^2 + x_{14}^2, \ldots, x_{n1}^2 + x_{n2}^2 + x_{n3}^2 + x_{n4}^2) = 0] \end{array} \right]$$

for all $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots]$. □

Note: Undecidability status of HTP for $\mathbb{Q}$ is still open!

Proof Idea

To compare equations and algorithms, we define the two classes of sets Diophantine sets and c.e. sets from each notions.

$$\{\text{Diophantine equations}\} \qquad \{\text{Turing machines}\}$$

$$\text{existence of solution} \downarrow \qquad \text{termination of computation} \downarrow$$

$$\{\text{Diophantine sets} \subseteq \mathbb{N}^n\} \qquad \{\text{c.e. sets} \subseteq \mathbb{N}^n\}$$

Then our goal is to prove that the equality of the two classes.

Proof Idea

To compare equations and algorithms, we define the two classes of sets Diophantine sets and c.e. sets from each notions.

$$\begin{array}{ccc} \{\text{Diophantine equations}\} & & \{\text{Turing machines}\} \\ \text{existence of solution}\downarrow & & \text{termination of computation}\downarrow \\ \{\text{Diophantine sets} \subseteq \mathbb{N}^n\} & = & \{\text{c.e. sets} \subseteq \mathbb{N}^n\} \end{array}$$

Then our goal is to prove that the equality of the two classes.

Diophantine Sets

Definition

A set of n-tuples $D \subseteq \mathbb{N}^n$ is Diophantine if there exists a polynomial $f(\vec{a}, \vec{x}) \in \mathbb{Z}[a_1, \ldots, a_n, x_1, \ldots, x_m]$ such that

$$D = \{\, \vec{a} \in \mathbb{N}^n \mid \exists \vec{x} \in \mathbb{N}^m [f(\vec{a}, \vec{x}) = 0] \,\}.$$

An n-ary relation $R(a_1, \ldots, a_n)$ is Diophantine if it is a Diophantine as a subset of $\mathbb{N}^n$. An n-ary function $f(a_1, \ldots, a_n)$ is Diophantine if its graph is a Diophantine subset of $\mathbb{N}^{n+1}$.

Example

- $\{0, 2, 4, 6, \ldots\} = \{\, a \in \mathbb{N} \mid \exists x \in \mathbb{N}[a = 2x] \,\}$,
- $a \mid b \iff \exists x \in \mathbb{N}[ax = b]$,
- $a < b \iff \exists x \in \mathbb{N}[b = a + x + 1]$.

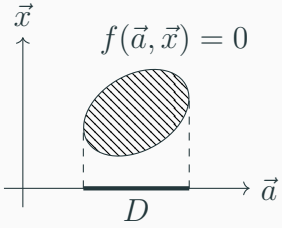
Diophantine Sets

Definition

A set of n-tuples $D \subseteq \mathbb{N}^n$ is Diophantine if there exists a polynomial $f(\vec{a}, \vec{x}) \in \mathbb{Z}[a_1, \ldots, a_n, x_1, \ldots, x_m]$ such that

$$D = \{\, \vec{a} \in \mathbb{N}^n \mid \exists \vec{x} \in \mathbb{N}^m [f(\vec{a}, \vec{x}) = 0] \,\}.$$

An n-ary relation $R(a_1, \ldots, a_n)$ is Diophantine if it is a Diophantine as a subset of $\mathbb{N}^n$. An n-ary function $f(a_1, \ldots, a_n)$ is Diophantine if its graph is a Diophantine subset of $\mathbb{N}^{n+1}$.



Example

- $\{0, 2, 4, 6, \ldots\} = \{\, a \in \mathbb{N} \mid \exists x \in \mathbb{N}[a = 2x] \,\}$,
- $a \mid b \iff \exists x \in \mathbb{N}[ax = b]$,
- $a < b \iff \exists x \in \mathbb{N}[b = a + x + 1]$.

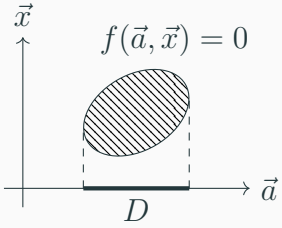
Diophantine Sets

Definition

A set of n-tuples $D \subseteq \mathbb{N}^n$ is Diophantine if there exists a polynomial $f(\vec{a}, \vec{x}) \in \mathbb{Z}[a_1, \ldots, a_n, x_1, \ldots, x_m]$ such that

$$D = \{\, \vec{a} \in \mathbb{N}^n \mid \exists \vec{x} \in \mathbb{N}^m [f(\vec{a}, \vec{x}) = 0] \,\}.$$

An n-ary relation $R(a_1, \ldots, a_n)$ is Diophantine if it is a Diophantine as a subset of $\mathbb{N}^n$. An n-ary function $f(a_1, \ldots, a_n)$ is Diophantine if its graph is a Diophantine subset of $\mathbb{N}^{n+1}$.



Example

- $\{0, 2, 4, 6, \ldots\} = \{\, a \in \mathbb{N} \mid \exists x \in \mathbb{N}[a = 2x] \,\}$,
- $a \mid b \iff \exists x \in \mathbb{N}[ax = b]$,
- $a < b \iff \exists x \in \mathbb{N}[b = a + x + 1]$.

C.E. Sets

Definition

A set of n-tuples $C \subseteq \mathbb{N}^n$ is computably enumerable (c.e.) if C satisfies one of the following equivalent conditions.

1. C is the domain of a partial computable function from $\mathbb{N}^n$ to $\mathbb{N}$.
2. $C = \emptyset$ or C is the range of a total computable function from $\mathbb{N}$ to $\mathbb{N}^n$. That is, C is "listable" set.

It is well known that the halting problem is c.e. but not computable.

Problem (Halting Problem)

Input: *A Turing machine M and $x \in \mathbb{N}$*

Question: *Does M eventually halt on the input x?*

It is easy to see that every Diophantine set is a c.e. set.

C.E. Sets

Definition

A set of n-tuples $C \subseteq \mathbb{N}^n$ is computably enumerable (c.e.) if C satisfies one of the following equivalent conditions.

1. C is the domain of a partial computable function from $\mathbb{N}^n$ to $\mathbb{N}$.
2. $C = \emptyset$ or C is the range of a total computable function from $\mathbb{N}$ to $\mathbb{N}^n$. That is, C is "listable" set.

It is well known that the halting problem is c.e. but not computable.

Problem (Halting Problem)

Input: *A Turing machine M and $x \in \mathbb{N}$*

Question: *Does M eventually halt on the input x?*

It is easy to see that every Diophantine set is a c.e. set.

C.E. Sets

Definition

A set of n-tuples $C \subseteq \mathbb{N}^n$ is computably enumerable (c.e.) if C satisfies one of the following equivalent conditions.

1. C is the domain of a partial computable function from $\mathbb{N}^n$ to $\mathbb{N}$.
2. $C = \emptyset$ or C is the range of a total computable function from $\mathbb{N}$ to $\mathbb{N}^n$. That is, C is "listable" set.

It is well known that the halting problem is c.e. but not computable.

Problem (Halting Problem)

Input: *A Turing machine M and $x \in \mathbb{N}$*

Question: *Does M eventually halt on the input x?*

It is easy to see that every Diophantine set is a c.e. set.

MRDP theorem

Now we can explain the precise form of the theorem by Matiyasevich, which based on the works of Robinson, Davis and Putnam.

Theorem (Matiysevich-Robinson-Davis-Putnam; MRDP theorem)

Every c.e. set is Diophantine.

Proof of MRDP theorem

The proof of MRDP theorem by Matiyasevich proceeds as follows.

1. Prove some closure properties of the class of the Diophantine sets.
2. Prove that $a = b^c$ is Diophantine.
3. Develop technique of coding of finite sequenes.
4. Simulate the computation of a Turing machine with Diophantine relations.

Some Closure Properties of the Diophantine Sets

Proposition

Let $R_1(a_1, \ldots, a_n), R_2(a_1, \ldots, a_n) \subseteq \mathbb{N}^n$ are Diophantine sets. Then the following are also Diophantine.

1. $(R_1 \vee R_2)(a_1, \ldots, a_n)$,
2. $(R_1 \wedge R_2)(a_1, \ldots, a_n)$,
3. $\exists x_i R_1(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$.

Proof.

Let $f_i(\vec{a}, \vec{x}_i)$ be a polynomial such that $R_i(\vec{a}) \iff \exists \vec{x}_i[f(\vec{a}, \vec{x}_i) = 0]$ for $i = 1, 2$. Then

1. $(R_1 \vee R_2)(\vec{a}) \iff \exists \vec{x}_1 \exists \vec{x}_2[f_1(\vec{a}, \vec{x}_1) \cdot f_2(\vec{a}, \vec{x}_2) = 0]$.
2. $(R_1 \wedge R_2)(\vec{a}) \iff \exists \vec{x}_1 \exists \vec{x}_2[f_1(\vec{a}, \vec{x}_1)^2 + f_2(\vec{a}, \vec{x}_2)^2 = 0]$.
3. Obvious.

Some Closure Properties of the Diophantine Sets

Proposition

Let $R_1(a_1, \ldots, a_n), R_2(a_1, \ldots, a_n) \subseteq \mathbb{N}^n$ are Diophantine sets. Then the following are also Diophantine.

1. $(R_1 \vee R_2)(a_1, \ldots, a_n)$,
2. $(R_1 \wedge R_2)(a_1, \ldots, a_n)$,
3. $\exists x_i R_1(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$.

Proof.

Let $f_i(\vec{a}, \vec{x}_i)$ be a polynomial such that $R_i(\vec{a}) \iff \exists \vec{x}_i[f(\vec{a}, \vec{x}_i) = 0]$ for $i = 1, 2$. Then

1. $(R_1 \vee R_2)(\vec{a}) \iff \exists \vec{x}_1 \exists \vec{x}_2[f_1(\vec{a}, \vec{x}_1) \cdot f_2(\vec{a}, \vec{x}_2) = 0]$.
2. $(R_1 \wedge R_2)(\vec{a}) \iff \exists \vec{x}_1 \exists \vec{x}_2[f_1(\vec{a}, \vec{x}_1)^2 + f_2(\vec{a}, \vec{x}_2)^2 = 0]$.
3. Obvious.

□

Exponentiation is Diophantine

In fact, Matiyasevich proved that the binary exponential function $a = b^c$ is a Diophantine function.

Theorem (Matiyasevich, 1970)

The binary function $a = b^c$ is Diophantine, i.e., the set

$$\{\, (a, b, c) \in \mathbb{N}^3 \mid a = b^c \,\}$$

is Diophantine.

The proof of this theorem is too complicated, so we omit the proof here.

Coding Finite Sequences

We can manimuplate finite sequence with arbitrary length through the technique of positional coding.

Definition

A triple (a, b, c) is a positional code of a sequence $(a_1, \ldots, a_c)$ if

1. $b \geq 2$ and $a_i < b$ for $i = 1, \ldots, c$,
2. $a = a_c b^{c-1} + a_{c-1} b^{c-2} + \cdots + a_2 b + a_1$.

By taking advantage of exponential function, we can develop Diophantine functions/relations such as

- d-th element of tuple with code (a, b, c),
- (a, b, c) is a code of concatenation of two sequences whose code are (a_1, b_1, c_1), (a_2, b_2, c_2), respectively.
- etc.

Coding Finite Sequences

We can manimuplate finite sequence with arbitrary length through the technique of positional coding.

Definition

A triple (a, b, c) is a positional code of a sequence $(a_1, \ldots, a_c)$ if

1. $b \geq 2$ and $a_i < b$ for $i = 1, \ldots, c$,
2. $a = a_c b^{c-1} + a_{c-1} b^{c-2} + \cdots + a_2 b + a_1$.

By taking advantage of exponential function, we can develop Diophantine functions/relations such as

- d-th element of tuple with code (a, b, c),
- (a, b, c) is a code of concatenation of two sequences whose code are (a_1, b_1, c_1), (a_2, b_2, c_2), respectively.
- etc.

Table of Contents

Elimination of Bounded Universal Quantifiers

Theorem

For any $(n+1)$-ary Diophantine relation $R(a_0, a_1 \ldots, a_n)$, the $(n+1)$-ary relation

$$\forall x < a_0[R(x, a_1, \ldots, a_n)] \qquad (*)$$

is also Diophantine.

Proof.

Let M be a Turing machine such that $\mathrm{dom}(M) = R$. Let N be the Turing machine which simulate the computations

$$M(0, a_1, \ldots, a_n), \ldots, M(a_0 - 1, a_1, \ldots, a_n)$$

simultaneously. Then $\mathrm{dom}(N)$ coinside with $(*)$. □

Elimination of Bounded Universal Quantifiers

Theorem

For any $(n+1)$-ary Diophantine relation $R(a_0, a_1 \ldots, a_n)$, the $(n+1)$-ary relation

$$\forall x < a_0[R(x, a_1, \ldots, a_n)] \qquad (*)$$

is also Diophantine.

Proof.

Let M be a Turing machine such that $\mathrm{dom}(M) = R$. Let N be the Turing machine which simulate the computations

$$M(0, a_1, \ldots, a_n), \ldots, M(a_0 - 1, a_1, \ldots, a_n)$$

simultaneously. Then $\mathrm{dom}(N)$ coinside with $(*)$. □

Goldbach Conjecture

Goldbach's conjecture is one of the open problems in number theory.

Conjecture

Any even integer $n \geq 4$ can be expressed as the sum of two prime numbers.

Failing the conjecture is equivalent to that there exists an even integer $2a+4$ $(a \geq 0)$ such that

$$\forall z < a+1 \exists x \exists y [z+2 = (x+2)(y+2) \vee (2a+4) - (z+2) = (x+2)(y+2)]. \quad (\sharp)$$

Since $\exists x \exists y [\cdots]$ is Diophantine relation, eliminating bounded universal quantifier from $(\sharp)$ yields a polynomial $f(a, \vec{x}) \in \mathbb{Z}[a, \vec{x}]$ such that

$2a+4$ is a counterexample of Goldbach conjecture $\iff \exists \vec{x} \in \mathbb{N}^n [f(a, \vec{x}) = 0]$.

Thus we have

$$\text{Goldbach conjecture} \iff \neg \exists a \in \mathbb{N} \exists \vec{x} \in \mathbb{N}^n [f(a, \vec{x}) = 0].$$

Goldbach Conjecture

Goldbach's conjecture is one of the open problems in number theory.

Conjecture

Any even integer $n \geq 4$ can be expressed as the sum of two prime numbers.

Failing the conjecture is equivalent to that there exists an even integer $2a + 4$ ($a \geq 0$) such that

$$\forall z < a + 1 \exists x \exists y [z + 2 = (x + 2)(y + 2) \vee (2a + 4) - (z + 2) = (x + 2)(y + 2)]. \quad (\sharp)$$

Since $\exists x \exists y [\cdots]$ is Diophantine relation, eliminating bounded universal quantifier from ($\sharp$) yields a polynomial $f(a, \vec{x}) \in \mathbb{Z}[a, \vec{x}]$ such that

$2a + 4$ is a counterexample of Goldbach conjecture $\iff \exists \vec{x} \in \mathbb{N}^n [f(a, \vec{x}) = 0]$.

Thus we have

$$\text{Goldbach conjecture} \iff \neg \exists a \in \mathbb{N} \exists \vec{x} \in \mathbb{N}^n [f(a, \vec{x}) = 0].$$

Goldbach Conjecture

Goldbach's conjecture is one of the open problems in number theory.

Conjecture

Any even integer $n \geq 4$ can be expressed as the sum of two prime numbers.

Failing the conjecture is equivalent to that there exists an even integer $2a + 4$ ($a \geq 0$) such that

$$\forall z < a + 1 \exists x \exists y [z + 2 = (x + 2)(y + 2) \vee (2a + 4) - (z + 2) = (x + 2)(y + 2)]. \quad (\sharp)$$

Since $\exists x \exists y [\cdots]$ is Diophantine relation, eliminating bounded universal quantifier from ($\sharp$) yields a polynomial $f(a, \vec{x}) \in \mathbb{Z}[a, \vec{x}]$ such that

$2a + 4$ is a counterexample of Goldbach conjecture $\iff \exists \vec{x} \in \mathbb{N}^n [f(a, \vec{x}) = 0]$.

Thus we have

$$\text{Goldbach conjecture} \iff \neg \exists a \in \mathbb{N} \exists \vec{x} \in \mathbb{N}^n [f(a, \vec{x}) = 0].$$

Goldbach Conjecture

Goldbach's conjecture is one of the open problems in number theory.

Conjecture

Any even integer $n \geq 4$ can be expressed as the sum of two prime numbers.

Failing the conjecture is equivalent to that there exists an even integer $2a + 4$ ($a \geq 0$) such that

$$\forall z < a + 1 \exists x \exists y [z + 2 = (x + 2)(y + 2) \vee (2a + 4) - (z + 2) = (x + 2)(y + 2)]. \quad (\sharp)$$

Since $\exists x \exists y [\cdots]$ is Diophantine relation, eliminating bounded universal quantifier from ($\sharp$) yields a polynomial $f(a, \vec{x}) \in \mathbb{Z}[a, \vec{x}]$ such that

$2a + 4$ is a counterexample of Goldbach conjecture $\iff \exists \vec{x} \in \mathbb{N}^n [f(a, \vec{x}) = 0]$.

Thus we have

$$\text{Goldbach conjecture} \iff \neg \exists a \in \mathbb{N} \exists \vec{x} \in \mathbb{N}^n [f(a, \vec{x}) = 0].$$

Diophantine Equation Representing the Inconsistency of ZFC

One can construct a Turing machine M such that

for any input $x = \ulcorner \varphi \urcorner$, M searches a proof of φ from ZFC.

It follows from MRDP theorem that there exists a polynomial $f(a, \vec{x})$ such that

$$\forall a \in \mathbb{N}(M(a)\downarrow \iff \exists \vec{x} \in \mathbb{N}^n[f(a, \vec{x}) = 0]).$$

In particular we have

$$\neg\, \mathrm{Con(ZFC)} \iff M(\ulcorner \bot \urcorner)\downarrow \iff \exists \vec{x} \in \mathbb{N}^n[f(\ulcorner \bot \urcorner, \vec{x}) = 0].$$

Thus, if $\mathrm{Con(ZFC)}$, then we cannot prove that the equation $f(\ulcorner \bot \urcorner, \vec{x}) = 0$ has no solution, while it actually has no solution.

Diophantine Equation Representing the Inconsistency of ZFC

One can construct a Turing machine M such that

for any input $x = \ulcorner \varphi \urcorner$, M searches a proof of φ from ZFC.

It follows from MRDP theorem that there exists a polynomial $f(a, \vec{x})$ such that

$$\forall a \in \mathbb{N}(M(a)\downarrow \iff \exists \vec{x} \in \mathbb{N}^n[f(a, \vec{x}) = 0]).$$

In particular we have

$$\neg\, \mathrm{Con(ZFC)} \iff M(\ulcorner \bot \urcorner)\downarrow \iff \exists \vec{x} \in \mathbb{N}^n[f(\ulcorner \bot \urcorner, \vec{x}) = 0].$$

Thus, if $\mathrm{Con(ZFC)}$, then we cannot prove that the equation $f(\ulcorner \bot \urcorner, \vec{x}) = 0$ has no solution, while it actually has no solution.

Diophantine Equation Representing the Inconsistency of ZFC

One can construct a Turing machine M such that

for any input $x = \ulcorner \varphi \urcorner$, M searches a proof of φ from ZFC.

It follows from MRDP theorem that there exists a polynomial $f(a, \vec{x})$ such that

$$\forall a \in \mathbb{N}(M(a)\downarrow \iff \exists \vec{x} \in \mathbb{N}^n[f(a, \vec{x}) = 0]).$$

In particular we have

$$\neg\, \mathrm{Con}(\mathsf{ZFC}) \iff M(\ulcorner \bot \urcorner)\downarrow \iff \exists \vec{x} \in \mathbb{N}^n[f(\ulcorner \bot \urcorner, \vec{x}) = 0].$$

Thus, if $\mathrm{Con}(\mathsf{ZFC})$, then we cannot prove that the equation $f(\ulcorner \bot \urcorner, \vec{x}) = 0$ has no solution, while it actually has no solution.

References

- A. R. Booker, *Cracking the problem with 33*, arXiv Preprint, `https://arxiv.org/abs/1903.04284`.
- Y. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press, 1993.
- M. Sipser, *Introduction to the Theory of Computation*, Third Edition, Cengage Learning, 2012.