An on-line talk invited by Shandong Univ. (Aug. 13, 2021)

Hilbert's Tenth Problem and its Further Developments

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://maths.nju.edu.cn/∼zwsun

August 13, 2021

Abstract

Hilbert's Tenth Problem (HTP) asks for an effective algorithm to decide whether an arbitrary polynomial equation

$$P(x_1, \ldots, x_n) = 0$$

(with integer coefficients) has integer solutions. This was finally solved by Matiyasevich in 1970 negatively.

In this talk we review the history of HTP and also introduce its further developments.

Part I. History of Hilbert's Tenth Problem (HTP)

Hilbert's Tenth Problem

In 1900, at the Paris conference of ICM, D. Hilbert presented 23 famous mathematical problems. Many of them are questions of others, however the tenth one is due to Hilbert himself.

In modern language, **Hilbert's Tenth Problem (HTP)** asks for an effective algorithm to test whether an arbitrary polynomial equation

$$P(z_1, \ldots, z_n) = 0$$

(with integer coefficients) has solutions over the ring $\mathbb{Z}$ of the integers.

However, at that time the exact meaning of *algorithm* was not known.

Note that a system of finitely many Diophantine equations over $S \subseteq \mathbb{Z}$ is equivalent to a single Diophantine equation over S. In fact, if $P_i(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$ for all $i = 1, \ldots, k$, then

$$\begin{aligned} & P_1(z_1, \ldots, z_n) = 0 \wedge \ldots \wedge P_k(z_1, \ldots, z_n) = 0 \\ \iff & P_1^2(z_1, \ldots, z_n) + \ldots + P_k^2(z_1, \ldots, z_n) = 0. \end{aligned}$$

Partial recursive functions

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and call each $n \in \mathbb{N}$ a *natural number*.

Three Basic Functions:
Zero Function: $O(x) = 0$ (for all $x \in \mathbb{N}$).
Successor Function: $S(x) = x + 1$.
Projection Function: $I_{nk}(x_1, \ldots, x_n) = x_k$ $(1 \leqslant k \leqslant n)$

Composition:

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$$

Primitive Recursion:

$$\begin{cases} f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n), \\ f(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \end{cases}$$

μ-operator: $f(x_1, \ldots, x_n) = \mu y(g(x_1, \ldots, x_n, y) = 0)$ means that $f(x_1, \ldots, x_n)$ is the least $y \in \mathbb{N}$ with $g(x_1, \ldots, x_n, y) = 0$. If $g(x_1, \ldots, x_n, y) \neq 0$ for all $y \in \mathbb{N}$, then $f(x_1, \ldots, x_n)$ is undefined.

Partial recursive functions are the basic functions and those obtained from the basic functions by applying composition, primitive recursion and the μ-operator a finite number of times.

Turing machine

In 1936 A. Turing introduced the notion of Turing machine which is an abstract machine that manipulates symbols on a strip of tape according to a table of rules (i.e., a program) involving four kinds of basic operations: Write 1, change 1 to 0 (blank), move to the left unit (L), move to the right unit (R).

To input $x_1, \ldots, x_n \in \mathbb{N}$, we use $x_1 + 1$ consecutive $1s$, a blank unit, $x_2 + 1$ consecutive $1s$, a blank unit, ..., $x_n + 1$ consecutive $1s$.

A function $f(x_1, \ldots, x_n)$ is *Turing computable* if there is a program according to which the Turing machine with initial inputs $x_1, \ldots, x_n$ finally stops and yields the value $f(x_1, \ldots, x_n)$ as outut if $f(x_1, \ldots, x_n)$ is defined, and never stops if $f(x_1, \ldots, x_n)$ is undefined.

A Turing program for $O(x) = 0$: $q_0 1 R q_1,\ q_1 1 0 q_2,\ q_2 0 R q_1$.

A Turing program for $S(x) = x + 1$: $q_0 1 L q_1,\ q_1 0 1 q_2$.

Partial recursive functions and Turing computable functions were proved to be equivalent by Kleene in 1936.

Church's Thesis

For any partial recursive function f, it is easy to see that if $f(x_1, \ldots, x_n)$ is defined then the value $f(x_1, \ldots, x_n)$ is effectively computable.

Church's Thesis (1936). If a function f into $\mathbb{N}$ with natural number variables is effectively computable by intuition, then it must be a partial recursive function (equivalently, a Turing computable function).

Nowadays, Church's Thesis is widely accepted. So we have the exact definition of computable functions (which refer to partial recursive functions or Turing computable functions).

Recursively enumerable sets

A subset A of $\mathbb{N}$ is said to be an *r.e. (recursively enumerable) set* (or *a semi-decidable set*) if the function

$$f_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ \text{undefined} & \text{if } x \in \mathbb{N} \setminus A. \end{cases}$$

is a partial recursive function.

If $A = \mathrm{Dom}(f)$ for some partial recursive function f, then we may revise the program computing $f(x)$ by letting the output be 1 if $f(x)$ is computed, and thus A is an r.e. set.

In view of the above,

$$\begin{aligned} & A \subseteq \mathbb{N} \text{ is an r.e. set} \\ \iff & A = \mathrm{Dom}(f) \text{ for some partial recursive function } f. \end{aligned}$$

Recursively enumerable sets

Suppose that A is an r.e. set containing an element a, and the Turing program P computes the function f_A. Then

$$g(x,y) = \begin{cases} x & \text{if the program } P \text{ computes } f_A(x) \text{ within } y \text{ steps,} \\ a & \text{otherwise} \end{cases}$$

is a total recursive function with $\mathrm{Ran}(g) = A$. If we define $F(2^x(2y+1)-1) = g(x,y)$ then F is a total recursive function with $\mathrm{Ran}(F) = \mathrm{Ran}(g) = A$ and thus $A = \{F(0), F(1), \ldots\}$.

If A is the range of a partial recursive function $h(x_1, \ldots, x_n)$, then the function

$$f(x) = \begin{cases} 1 & \text{if } x \in \mathrm{Ran}(h) = A, \\ \text{undefined} & \text{otherwise,} \end{cases}$$

is a partial recursive function (we may seek for $x_1, \ldots, x_n$ with $h(x_1, \ldots, x_n)$ equal to a given $x \in A$), and thus A is an r.e. set.

So, a nonempty $A \subseteq \mathbb{N}$ is an r.e. set if and only if $A = \mathrm{Ran}(f)$ for some total recursive function f.

r.e. sets and recursive sets

Enumeration Theorem (Kleene). There is a partial recursive function $\varphi(m, n)$ such that

$$\varphi_0, \varphi_1, \varphi_2, \ldots$$

list all the partial recursive functions of one variable. where φ_m is given by

$$\varphi_m(n) = \varphi(m, n) \ (n = 0, 1, 2, \ldots).$$

A set $A \subseteq \mathbb{N}$ is called *decidable* or *recursive*, if the characteristic function

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \in \mathbb{N} \setminus A. \end{cases}$$

is Turing computable (or recursive).

A set $A \subseteq \mathbb{N}$ is recursive if and only if both A and $\mathbb{N} \setminus A$ are r.e. sets.

Halting Problem is undecidable

Theorem. The set $K = \{x \in \mathbb{N} : \ x \in \mathrm{Dom}(\varphi_x)\}$ is a nonrecursive r.e. set.

Proof. As the function $\varphi_x(x) = \varphi(x, x)$ is a partial recursive function, we see that K is an r.e. set.

Suppose that K is recursive. Then the function

$$f(x) = \begin{cases} \varphi_x(x) + 1 & \text{if } x \in \mathrm{Dom}(\varphi_x), \\ 0 & \text{otherwise,} \end{cases}$$

is totally recursive, thus for some $m \in \mathbb{N}$ we have $\varphi_m = f$ and hence

$$f(m) = \varphi_m(m) \neq \varphi_m(m) + 1$$

which leads a contradiction.

Let P_x be a Turing program computing φ_x. Whether a Turing machine with input x and program P_x finally stops, is an undecidable problem which is called the halting problem.

Diophantine equations over $\mathbb{N}$ and $\mathbb{Z}$

Throughout this talk, variables range over $\mathbb{Z}$ unless specified.

Let $P(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$. Then

$$\begin{aligned} & \exists z_1 \ldots \exists z_n [P(z_1, \ldots, z_n) = 0] \\ \iff & \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 \left[\prod_{\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}} P(\varepsilon_1 x_1, \ldots, \varepsilon_n x_n) = 0 \right]. \end{aligned}$$

On the other hand, by Lagrange's four-square theorem (each $m \in \mathbb{N}$ can be written as the sum of four squares), we have

$$\begin{aligned} & \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [P(x_1, \ldots, x_n) = 0] \\ \iff & \exists u_1 \exists v_1 \exists y_1 \exists z_1 \ldots \exists u_n \exists v_n \exists y_n \exists z_n \\ & [P(u_1^2 + v_1^2 + y_1^2 + z_1^2, \ldots, u_n^2 + v_n^2 + y_n^2 + z_n^2) = 0] \end{aligned}$$

So HTP has the following equivalent form (HTP over $\mathbb{N}$): *Is there an algorithm to decide for any polynomial $P(x_1, \ldots, x_n)$ with integer coefficients whether the Diophantine equation $P(x_1, \ldots, x_n) = 0$ has solutions with $x_1, \ldots, x_n \in \mathbb{N}$?*

Diophantine relations and Diophantine sets

A relation $R(a_1, \ldots, a_m)$ with $a_1, \ldots, a_m \in \mathbb{N}$ is said to be *Diophantine* if there is a polynomial $P(t_1, \ldots, t_m, x_1, \ldots, x_n)$ with integer coefficients such that

$$R(a_1, \ldots, a_m) \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [P(a_1, \ldots, a_m, x_1, \ldots, x_n) = 0].$$

A set $A \subseteq \mathbb{N}$ is Diophantine if and only if the predicate $a \in A$ is Diophantine.

It is easy to see that any Diophantine set A is an r.e. set. In fact, for a given element $a \in A$ we may search for the natural number solutions of the related Diophantine equation. If it has a solution, then we will find one and let the computer stop and give the output 1. If it has no solution, the computer will never stop.

Davis Daring Hypothesis

In 1944 E. L. Post thought that HTP *begs for an unsolvability proof*, i.e., HTP might be undecidable.

In 1949 Martin Davis used Gödel's coding idea to obtain that any r.e. set $A \subseteq \mathbb{N}$ has the following Davis normal form

$$a \in A \iff \exists x \geqslant 0 \forall 0 \leqslant y \leqslant x \exists z_1 \geqslant 0 \ldots \exists z_n \geqslant 0$$
$$[P(a, x, y, z_1, \ldots, z_n) = 0],$$

where a is a natural number and P is a polynomial with integer coefficients.

Davis Daring Hypothesis. Any r.e. set $A \subseteq \mathbb{N}$ is Diophantine.

Under this hypothesis, for the nonrecursive r.e. set $K = \{x \in \mathbb{N} : \ x \in \mathrm{Dom}(\varphi_x)\}$ there is a polynomial $P(x, x_1, \ldots, x_n)$ such that for any $a \in \mathbb{N}$ we have

$$a \in K \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [P(a, x_1, \ldots, x_n) = 0].$$

Thus Davis Daring Hypothesis implies that HTP over $\mathbb{N}$ is undecidable.

Exponential Diophantine relations

Exponential Diophantine equations have the form

$$E_1(x_1, \ldots, x_m) = E_2(x_1, \ldots, x_m),$$

where E_1 and E_2 are expressions constructed from variables and particular natural numbers using addition, multiplication, and exponentiation. Here is an example of exponential Diophantine equation:

$$x^{2^y} + y^2 + y^{y^z} = 5z^{x^x+3z}.$$

A relation $R(a_1, \ldots, a_m)$ with $a_1, \ldots, a_m \in \mathbb{N}$ is said to be *exponential Diophantine* if there is an exponential Diophantine equation

$$E(t_1, \ldots, t_m, x_1, \ldots, x_n) = 0$$

such that

$$R(a_1, \ldots, a_m) \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [E(a_1, \ldots, a_m, x_1, \ldots, x_n) = 0].$$

A set $A \subseteq \mathbb{N}$ is called exponential Diophantine if the predicate $a \in A$ is Diophantine.

J. Robinson: $z = \binom{n}{k}$ is exponential Diophantine

If $0 < k \leqslant n$ and $u > 2^n$, then

$$\frac{(u+1)^n}{u^k} = \binom{n}{k} + u \sum_{k<m\leqslant n} \binom{n}{m} u^{m-k-1} + \sum_{0\leqslant i<k} \binom{n}{i} \frac{u^i}{u^k}$$

by the binomial theorem, hence

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv \binom{n}{k} \pmod{u}$$

and thus $\binom{n}{k}$ is the least nonnegative residue of $\lfloor (u+1)^n / u^k \rfloor$ modulo u.

For $z \geqslant 0$ and $n \geqslant k > 0$, the relation $z = \binom{n}{k}$ holds if and only if there are $u, v, w, x, y \in \mathbb{N}$ such that

$$u > v,\ v = 2^n,\ z = \mathrm{rem}(w, u),$$
$$x = (u+1)^n,\ y = u^k,\ yw \leqslant x < (w+1)y.$$

$z = n!$ is exponential Diophantine

If $n > 0$ and $m > (2n)^{n+1}$, then

$$n! < \frac{m^n}{\binom{m}{n}} = \frac{n!}{\prod_{r=1}^{n-1}(1 - r/m)} < \frac{n!}{(1 - n/m)^n} < n! \left(1 + \frac{2n}{m}\right)^n < n!+1$$

and thus $n! = \lfloor m^n / \binom{m}{n} \rfloor$.

For $z \geqslant 0$ and $n > 0$, the relation $z = n!$ holds if and only if there are $u, v, w, x, y \in \mathbb{N}$ such that

$$u > v,\ v = w^{n+1},\ w = 2n,\ x = u^n,\ y = \binom{u}{n},\ yz \leqslant x < (z+1)y.$$

Therefore, $z = n!$ is exponential Diophantine!

The Davis-Putnam-Robinson theorem

Theorem (M. Davis, H. Putnam, J. Robinson, Annals of Math. 1961) Any r.e. set is exponential Diophantine. Thus there is no algorithm to decide for any given exponential Diophantine equation whether it has solutions over $\mathbb{N}$.

Davis-Putnam-Robinson Lemma. Let $b \in \{2, 3, \ldots\}$, $P(y, x_1, \ldots, x_m) \in \mathbb{Z}[y, x_1, \ldots, x_m]$, and $B(b, w) = P^*(b, w, \ldots, w)$ with $P^*(y, x_1, \ldots, x_m)$ obtained by replacing each coefficient in $P(y, x_1, \ldots, x_m)$ by its absolute value. Then

$$\forall 0 \leqslant y < b \exists x_1 \geqslant 0 \ldots \exists x_m \geqslant 0 [P(y, x_1, \ldots, x_m) = 0]$$

$\iff$ there exist $q, w, z_1, \ldots, z_m \in \mathbb{N}$ such that

$$q \equiv -1 \pmod{b!(b + w + B(b, w))!}, \text{ and}$$

$$\binom{q}{b} \text{ divides } \binom{z_1}{w}, \ldots, \binom{z_m}{w} \text{ and } P(q, z_1, \ldots, z_m).$$

Remark. This is not the original form of the DPR Lemma, but a revised version by Y. Matiyasevich using the same ideas.

Sketch of the proof of the DPR theorem

Clearly the empty set $\emptyset$ is Diophantine since
$a \in \emptyset \iff \exists x \geqslant 0[x + 1 = 0]$.

Recall that a nonempty $A \subseteq \mathbb{N}$ is an r.e. set if and only if $A = \mathrm{Ran}(f)$ for some total recursive function f. So, it suffices to prove that for any total recursive function $f(x_1, \ldots, x_n)$ the relation $y = f(x_1, \ldots, x_n)$ is exponential Diophantine.

When

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)),$$

we have

$$y = f(x_1, \ldots, x_n) \iff \exists y_1 \geqslant 0 \ldots \exists y_m \geqslant 0[y = g(y_1, \ldots, y_m) \wedge y_1 = h(x_1, \ldots, x_n) \wedge \ldots \wedge y_m = h(x_1, \ldots, x_n)].$$

So, if $y = g(y_1, \ldots, y_m)$ and $y_i = h_i(x_1, \ldots, x_n)$ $(i = 1, \ldots, m)$ are all exponential Diophantine then $y = f(x_1, \ldots, x_n)$ is exponential Diophantine.

Deal with the μ-operator

When

$$f(x_1, \ldots, x_n) = \mu y[g(x_1, \ldots, x_n, y) = 0],$$

we have

$$\begin{aligned} & y = f(x_1, \ldots, x_n) \\ \Longleftrightarrow\ & g(x_1, \ldots, x_n, y) = 0 \wedge \forall 0 \leqslant z < y \exists x \geqslant 0[g(x_1, \ldots, x_n, z) = x + 1]. \end{aligned}$$

So, if $w = g(x_1, \ldots, x_n, z)$ is exponential Diophantine then $y = f(x_1, \ldots, x_n)$ is exponential Diophantine with the aid of the DPR lemma.

By induction, $y = f(x_1, \ldots, x_n)$ is exponential Diophantine for any total recursive function. So, any r.e. set is exponential Diophantine!

Julia Robinson's Hypothesis

A. Tarski conjectured in 1948 that $\{2^n : \ n \in \mathbb{N}\}$ is not a Diophantine set. His PhD student J. Robinson did not succeed in proving this with serious efforts.

JR Hypothesis (J. Robinson, 1950). There is a Diophantine relation $R(a, b)$ with $a, b \in \mathbb{N}$ such that

$$R(a, b) \Rightarrow b < a^a$$

and

$$\forall k > 0 \exists a \geqslant 0 \exists b \geqslant 0 [R(a, b) \ \& \ a^k < b].$$

Under this hypothesis, J. Robinson showed that the exponential relation $a^b = c$ is Diophantine and hence all r.e. sets are Diophantine. So, the JR Hypothesis implies the negative solution of HTP.

J. Robinson tried to prove her JR Hypothesis but got no success. This made her depressed and doubt her Hypothesis.

Davis' approach

In 1968 M. Davis showed that if the equation

$$9(u^2+7v^2)^2-7(x^2+7y^2)^2=2\ (u,v,x,y\in\mathbb{N})$$

only has finitely many solutions then the relation $a^b=c$ is Diophantine.

In 1972, Shanks found the first nontrivial solution of the equation with

$$u=525692038369576,\ v=155632703919101 3,$$
$$x=2484616164142152,\ y=1381783865776981.$$

Up to now, nobody can show that the Diophantine equation

$$9(u^2+7v^2)^2-7(x^2+7y^2)^2=2\ (u,v,x,y\in\mathbb{N})$$

only has finitely many solutions.

Matiyasevich's Theorem

Recall that the Fibonacci sequence $(F_n)_{n\geqslant 0}$ defined by

$$F_0 = 0,\ F_1 = 1,\ \text{ and } F_{n+1} = F_n + F_{n-1}\ (n = 1, 2, 3, \ldots)$$

increases exponentially.
In 1970 Yu. Matiyasevich, a 23-year-old Russian, confirmed the JR Hypothesis by showing that the relation $y = F_{2x}$ (with $x, y \in \mathbb{N}$) is Diophantine! It follows the exponential relation $a^b = c$ (with $a, b, c \in \mathbb{N}$, $a > 1$ and $c > 0$) is Diophantine, i.e. there exists a polynomial $P(a, b, c, x_1, \ldots, x_n)$ with integer coefficients such that

$$a^b = c \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0[P(a, b, c, x_1, \ldots, x_n) = 0].$$

This, together with the Davis-Putnam-Robinson work in 1961, led Matiyasevich finally confirm Davis Daring Hypothesis.

Matiyasevich's Theorem (or MDPR Theorem) (1970).
Recursively enumerable sets coincide with Diophantine sets. Thus HTP has a negative solution!

Part II. The 9 unknowns theorem and the 11 unknowns theorem

Small ν with $\exists^\nu$ over $\mathbb{N}$ undecidable

For a set $S \subseteq \mathbb{Z}$ we let $\exists^n$ over S denote the set of formulas

$$\exists x_1 \in S \ldots \exists x_n \in S[P(x_1, \ldots, x_n) = 0]$$

with $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$.

Any nonrecursive r.e. set A has a Diophantine representation:

$$a \in A \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0[P(x_1, \ldots, x_n) = 0].$$

It is interesting to find the least $\nu \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ such that $\exists^\nu$ over $\mathbb{N}$ is undecidable.

$\nu < 200$ (Matiyasevich, Summer of 1970)
$\nu \leqslant 35$ (J. Robinson, 1970)
$\nu \leqslant 24$ (Matiyasevich and Robinson, 1970)
$\nu \leqslant 14$ (Matiyasevich and Robinson, 1970)
$\nu \leqslant 13$ (Matiyasevich and Robinson, 1973 [Acta Arith. 27(1975)])
$\nu \leqslant 9$ (Matiyasevich, 1975; details in Jones [J. Symbolic Logic, 1982])

A useful lemma

Let $\square = \{x^2 : \ x \in \mathbb{N}\}$ and $A_1, \ldots, A_k \in \mathbb{Z}$. Then

$$\begin{aligned} & A_1, \ldots, A_k \in \square \\ \iff & \exists x_1 \geqslant 0 \ldots \exists x_k \geqslant 0 (x_1^2 = A_1 \wedge \ldots \wedge x_k^2 = A_k) \\ \iff & \exists x_1 \geqslant 0 \ldots \exists x_k \geqslant 0 [(x_1^2 - A_1)^2 + \ldots + (x_k^2 - A_k)^2 = 0]. \end{aligned}$$

To reduce the number of unknowns needed, Matiyasevich and J. Robinson found the following lemma.

A useful lemma

Let $\square = \{x^2 : \ x \in \mathbb{N}\}$ and $A_1, \ldots, A_k \in \mathbb{Z}$. Then

$$\begin{aligned} & A_1, \ldots, A_k \in \square \\ \iff & \exists x_1 \geqslant 0 \ldots \exists x_k \geqslant 0 (x_1^2 = A_1 \wedge \ldots \wedge x_k^2 = A_k) \\ \iff & \exists x_1 \geqslant 0 \ldots \exists x_k \geqslant 0 [(x_1^2 - A_1)^2 + \ldots + (x_k^2 - A_k)^2 = 0]. \end{aligned}$$

To reduce the number of unknowns needed, Matiyasevich and J. Robinson found the following lemma.

Lemma (Matiyasevich-Robinson [Acta Arith. 27(1975)]). The polynomial $J_k(x_1, \ldots, x_k, x)$ given by

$$\prod_{\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}} \left(x + \varepsilon_1 \sqrt{x_1} + \varepsilon_2 \sqrt{x_2} X + \ldots + \varepsilon_k \sqrt{x_k} X^{k-1} \right).$$

with $X = 1 + \sum_{j=1}^{k} x_j^2$ has integer coefficients. Moreover, $A_1, \ldots, A_k \in \mathbb{Z}$ are all squares if and only if $J_k(A_1, \ldots, A_k, x) = 0$ for some $x \in \mathbb{N}$.

This can be proved by induction on k and using Galois theory.

Matiyasevich-Robinson's Relation-Combining Theorem

Matiyasevich-Robinson's Relation-Combining Theorem [Acta Arith. 27(1975)] Let $A_1, \ldots, A_k$ and R, S, T be integers with $S \neq 0$. Then

$$\begin{aligned} & A_1 \in \square \wedge \ldots \wedge A_k \in \square \wedge S \mid T \wedge R > 0 \\ \iff & \exists n \geqslant 0 [M_k(A_1, \ldots, A_k, S, T, R, n) = 0], \end{aligned}$$

where $\square = \{x^2 : \ x \in \mathbb{N}\}$, and

$$\begin{aligned} & M_k(x_1, \ldots, x_k, w, x, y, z) \\ = & \prod_{\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}} \left(x^2 + w^2 z - w^2(2y-1)\left(x^2 + X^k + \sum_{j=1}^{k} \varepsilon_j \sqrt{x_j} X^{j-1} \right) \right) \\ = & (w^2(1-2y))^{2^k} J_k\left(x_1, \ldots, x_k, x^2 + X^k + \frac{x^2 + w^2 z}{w^2(1-2y)} \right) \end{aligned}$$

with $X = 1 + \sum_{j=1}^{k} x_j^2$, and $J_k(x_1, \ldots, x_k, x)$ being

$$\prod_{\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}} \left(x + \varepsilon_1 \sqrt{x_1} + \varepsilon_2 \sqrt{x_2} X + \ldots + \varepsilon_k \sqrt{x_k} X^{k-1} \right).$$

Proof of the Relation-Combining Theorem

Let $W = 1 + \sum_{j=1}^{k} A_j^2$. Recall that

$$\begin{aligned} &M_k(A_1, \ldots, A_k, S, T, R, n) \\ =&(S^2(1-2R))^{2^k} J_k\left(A_1, \ldots, A_k, T^2 + W^k + \frac{S^2 n + T^2}{S^2(1-2R)}\right). \end{aligned}$$

If $A_1, \ldots, A_k \in \square$, $S \mid T$ and $R > 0$, then

$$\begin{aligned} n =&(2R-1)(T^2 + W^k - \sqrt{A_1} - \sqrt{A_2}W - \ldots - \sqrt{A_k}W^{k-1}) - \frac{T^2}{S^2} \\ \geqslant& T^2 + W^k - \sum_{i=0}^{k-1}(W-1)W^i - \frac{T^2}{S^2} \geqslant W^k - (W^k - 1) \geqslant 0 \end{aligned}$$

and $M_k(A_1, \ldots, A_k, S, T, R, n) = 0$.

Now suppose that $M_k(A_1, \ldots, A_k, S, T, R, n) = 0$ for some $n \in \mathbb{N}$. Then $\alpha = T^2 + W^k + (S^2 n + T^2)/(S^2(1-2R))$ is a rational zero of the monic polynomial $J_k(A_1, \ldots, A_k, x)$. As rational algebraic integers lie in $\mathbb{Z}$, we have $\alpha \in \mathbb{Z}$, hence $A_1, \ldots, A_k \in \square$ and $S \mid T$. As $\alpha \leqslant \sum_{i=0}^{k-1} \sqrt{A_i} W^{i-1} \leqslant W^k - 1$ and $n \geqslant 0$, we have $R > 0$.

Coding idea of Matiyasevich and Robinson (1975)

Let $b \in \mathbb{N}$, $\delta \in \mathbb{Z}^+$, and

$$P(z_0, \ldots, z_\nu) = \sum_{\substack{i_0, \ldots, i_\nu \in \mathbb{N} \\ i_0 + \ldots + i_\nu \leqslant \delta}} a_{i_0, \ldots, i_\nu} z_0^{i_0} \cdots z_\nu^{i_\nu}.$$

$$B > 2\delta!(1 + b^\delta)\left(1 + \sum_{i_0 + \ldots + i_\nu \leqslant \delta} a_{i_0, \ldots, i_\nu}^2\right),$$

$$D(x) = x^{(\delta+1)^{\nu+2}} + \sum_{i_0 + \ldots + i_\nu \leqslant \delta} c_{i_0, \ldots, i_\nu} a_{i_0, \ldots, i_\nu} x^{(\delta+1)^{\nu+1} - \sum_{s=0}^{\nu} i_s (\delta+1)^s}$$

with $c_{i_0, \ldots, i_\nu} = i_0! \ldots i_\nu! (\delta - i_0 - \ldots - i_\nu)!$. Then

$P(z_0, \ldots, z_\nu) = 0$ for some $z_0, \ldots, z_\nu \in [0, b]$

$\iff$ there is a number c of the form $1 + \sum_{i=0}^{\nu} c_i B^{(\delta+1)^i}$ with $c_i \in [0, b]$

such that the coefficient of $x^{(\delta+1)^{\nu+1}}$ in $\left(1 + \sum_{i=0}^{\nu} c_i x^{(\delta+1)^i}\right)^\delta D(x)$

is zero.

Matiyasevich's idea to use binary representations

For $a, b \in \mathbb{N}$ written in base p with p prime, let $\tau_p(a, b)$ denote the number of carries occurring in the addition of a and b. Kummer noted that $\tau_p(a, b) = \operatorname{ord}_p\binom{a+b}{a}$.

Let $b, B \in 2\uparrow = \{2^n : \ n \in \mathbb{N}\}$ with $b \leqslant B$. Let $\delta, \nu \in \mathbb{Z}^+$. For $c = \sum_{j=0}^{(\delta+1)^\nu} c_j B^j$ with $c_j \in [0, B)$, and $M = \sum_{j=0}^{(\delta+1)^\nu} m_j B^j$ with

$$m_j = \begin{cases} B - b & \text{if } j = (\delta+1)^s \text{ for some } s = 1, \ldots, k, \\ B - 1 & \text{otherwise,} \end{cases}$$

$$\tau_2(c, M) = 0 \iff \tau_2(c_j, m_j) = 0 \text{ for all } j = 0, \ldots, (\delta+1)^\nu$$

$$\iff c = \sum_{i=1}^{\nu} z_i B^{(\delta+1)^i} \text{ for some } z_1, \ldots, z_k \in [0, b)$$

If $N \in 2\uparrow$ and $S, T \in [0, N)$, then

$$\tau_2(S, T) = 0 \iff N^2 \mid \binom{2R}{R}$$

where $R = (N-1)((S+T+1)N + T + 1)$.

The 9 Unknowns Theorem

The above ideas, together with some other works in the 1975 paper of Matiyasevich and Robinson, led Mtijasevich obtain the following celebrated theorem.

Matiyasevich's 9 Unknowns Theorem: $\exists^9$ over $\mathbb{N}$ is undecidable!

The detailed proof of this theorem appeared in Jones [J. Symbolic Logic, 1982].

Up to now, no one has shown that $\exists^\nu$ over $\mathbb{N}$ is undecidable for some $\nu < 9$, although A.Baker, Matiyasevich and Robinson all believed that $\exists^3$ over $\mathbb{N}$ might be undecidable.

Putnam's trick

H. Putnam [J. Symbolic Logic 25(1960)]: Let $A \subseteq \mathbb{N}$. Suppose that for any $a \in \mathbb{N}$ we have

$$a \in A \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0[P(a, x_1, \ldots, x_n) = 0].$$

Then

$$A = \{\tilde{P}(x_0, x_1, \ldots, x_n) : \ x_0, \ldots, x_n \in \mathbb{N}\} \cap \mathbb{N},$$

where $\tilde{P}$ is a suitable polynomial with integer coefficients.

Proof. Define

$$\tilde{P}(x_0, x_1, \ldots, x_n) = (x_0 + 1)(1 - P(x_0, x_1, \ldots, x_n)^2) - 1.$$

If $x_0, \ldots, x_n \in \mathbb{N}$, then

$$\tilde{P}(x_0, x_1, \ldots, x_n) \geqslant 0 \iff P(x_0, \ldots, x_n) = 0 \Rightarrow \tilde{P}(x_0, \ldots, x_n) = x_0 \in A.$$

Thus

$$\begin{aligned} A =& \{x_0 \in \mathbb{N} : \ \exists x_1 \geqslant 0 \ldots, \exists x_n \geqslant 0[P(x_0, \ldots, x_n) = 0]\} \\ =& \{\tilde{P}(x_0, x_1, \ldots, x_n) : \ x_0, \ldots, x_n \in \mathbb{N}\} \cap \mathbb{N}. \end{aligned}$$

The set of all primes

By Wilson's theorem, an integer $p > 1$ is prime if and only if $(p-1)! \equiv -1 \pmod{p}$. In view of this, the set of all primes is Diophantine, and Matiyasevich obtained the following surprising result with the use of a Putnam trick.

Matiyasevich (1975): There is a polynomial $P(x_0, \ldots, x_9)$ with integer coefficients such that

$$\{P(x_0, x_1, \ldots, x_9) : \ x_0, \ldots, x_9 \in \mathbb{N}\} \cap \mathbb{N}$$

coincides the set of all primes.

Remark. This looks `incredible` to number theorists!

There is no non-constant polynomial $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $P(x_1, \ldots, x_n)$ with $x_1, \ldots, x_n \in \mathbb{N}$ are all primes. For, if $P(x_1, \ldots, x_n)$ is a prime p, then

$$P(x_1 + py_1, \ldots, x_n + py_n) \equiv 0 \pmod{p}$$

for all $y_1, \ldots, y_n \in \mathbb{N}$.

$\exists$ over $\mathbb{Z}$ is decidable

Matiyasevich and Robinson [Acta Arith. 27(1975)]: If $a_0, a_1, \ldots, a_n$ and z are integers with $a_0 z \neq 0$ and $\sum_{i=0}^{n} a_i z^{n-i} = 0$, then

$$|z|^n \leqslant |a_0 z^n| \leqslant \sum_{i=1}^{n} |a_i| \cdot |z|^{n-i} \leqslant \sum_{i=1}^{n} |a_i| \cdot |z|^{n-1}$$

and hence

$$|z| \leqslant \sum_{i=1}^{n} |a_i|.$$

Thus $\exists$ over $\mathbb{N}$ and $\exists$ over $\mathbb{Z}$ are decidable (in polynomial time).

It is not known whether $\exists^2$ over $\mathbb{Z}$ is decidable. But A. Baker proved in 1968 that if $P(x, y) \in \mathbb{Z}[x, y]$ is homogenous, irreducible and of degree at least three then for any $m \in \mathbb{Z}$ there is an effective algorithm to determine whether $P(x, y) = m$ for some $x, y \in \mathbb{Z}$.

Relative results

For any $m \in \mathbb{Z}$, by Lagrange's four-square theorem

$$m \geqslant 0 \iff \exists z_1 \exists z_2 \exists z_3 \exists z_4 [m = z_1^2 + z_2^2 + z_3^2 + z_4^2].$$

Thus

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{4n} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

By the Gauss-Legendre theorem on sums of three squares,

$$\mathbb{N} \setminus \{x^2 + y^2 + z^2 : \ x, y, z \in \mathbb{Z}\} = \{4^k(8l + 7) : \ k, l \in \mathbb{N}\}.$$

If $n \in \mathbb{N}$, then $4n + 1 = (2x)^2 + (2y)^2 + (2z + 1)^2$ for some $x, y, z \in \mathbb{Z}$, and hence $n = x^2 + y^2 + z^2 + z$. Thus, for any $m \in \mathbb{Z}$,

$$m \geqslant 0 \iff \exists x \exists y \exists z [m = x^2 + y^2 + z^2 + z].$$

It follows that

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{3n} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

Thus $\exists^{27}$ over $\mathbb{Z}$ is undecidable by the 9 unknowns theorem, as pointed out by S.P. Tung in [Japan J. Math., 11(1985)].

A new relation-combining theorem

Tung (1985) asked whether $\exists^\nu$ over $\mathbb{Z}$ is undecidable for some $\nu < 27$.

New Relation-Combining Theorem (Z.-W. Sun [Z. Math. Logik Grundlag. Math. 38(1992)]): Let $A_1, \ldots, A_k, B, C_1, \ldots, C_n, D, E$ be integers with $D \neq 0$. Then

$$\begin{aligned} & A_1, \ldots, A_k \in \square \wedge B \neq 0 \wedge C_1, \ldots, C_n \geqslant 0 \wedge D \mid E \\ \Longleftrightarrow\ & \exists z_1 \ldots \exists z_{n+2} [P(A_1, \ldots, A_k, B, C_1, \ldots, C_n, D, E, z_1, \ldots, z_{n+2}) = 0], \end{aligned}$$

where P is a suitable polynomial with integer coefficients.

This implies that

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{2n+2} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

So $\exists^{20}$ over $\mathbb{Z}$ is undecidable by the 9 unknowns theorem.

Two useful observations

To prove the New Relation-Combining Theorem we need two useful observations.

An Observation of Shih Ping Tung (1985): For any $m \in \mathbb{Z}$, we have

$$m \neq 0 \iff \exists x \exists y [m = (2x+1)(3y+1)].$$

Note that if $m \in \mathbb{Z} \setminus \{0\}$ then we can write $m = \pm 3^a(3y+1) = (2x+1)(3y+1)$ with $x, y \in \mathbb{Z}$.

If $d \in \mathbb{Z}^+$ is **not** a perfect square, then the Pell equation

$$y^2 - dx^2 = 1$$

has infinitely many integer solutions; in particular $dx^2 + 1 \in \square$ for some $x \in \mathbb{Z} \setminus \{0\}$.

In 1992, I made use of this fact from number theory.

An Observation. Let $m \in \mathbb{Z}$. Then

$$m \geqslant 0 \iff \exists x \neq 0((4m+2)x^2 + 1 \in \square).$$

The 11 Unknowns Theorem: $\exists^{11}$ over $\mathbb{Z}$ is undecidable

In 1992, I announced that $\exists^{11}$ **over** $\mathbb{Z}$ **is undecidable**.

To achieve this goal, unlike others I did not simply use the relative result, instead I adapt the deep proof of the 9 unknowns theorem and made suitable variants so that we can use integer variables instead of natural number variables.

My starting point is the use of Lucas sequences with integer indices instead of the usual natural number indices. I published this initial step in Sci. China Ser. A 35(1992).

The whole proof of the undecidability of $\exists^{11}$ over $\mathbb{Z}$ is very sophisticated. It appeared in my PhD thesis in 1992. During 1992-2016, despite that many mathematicians wanted to see my detailed proof, I did not write an English version of that, since I was frequently busy with my new discoveries.

After 25 years had passed, I finally spent time to write an English paper which contains the undecidability of $\exists^{11}$ over $\mathbb{Z}$ as well as my new discoveries related to HTP. The paper was posted to arXiv in 2017, and published in Sci. China Math. [64(2021), 281-306].

A lemma on Lucas sequences

For $A, B \in \mathbb{Z}$ the Lucas sequence $u_n = u_n(A, B)$ $(n \in \mathbb{N})$ and its companion $v_n = v_n(A, B)$ $(n \in \mathbb{N})$ are defined as follows:

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = Au_n - Bu_{n-1}\ (n = 1, 2, 3, \ldots);$$
$$v_0 = 2,\ v_1 = A,\ v_{n+1} = Av_n - Bv_{n-1}\ (n = 1, 2, 3, \ldots).$$

Lemma 1 (See, e.g., Sun [Sci. China Ser. A 35(1992)]). Let $A \in \{2, 3, \ldots\}$. Then

$$(A^2 - 4)x^2 + 4 = y^2 \wedge x \geqslant 0 \wedge y \geqslant 0$$

if and only if

$$x = u_n(A, 1) \text{ and } y = v_n(A, 1) \text{ for some } n \in \mathbb{N}.$$

Two other lemmas

Lemma 2 (Sun [Sci. China Ser. A 35(1992)]). Let $A, B \in \mathbb{Z}$ with $|A| \geqslant 2$ and $B > 0$, and let $C = u_B(A, 1)$. Then $|C| \geqslant B$, and $DFI \in \square$ for some $x \neq 0$ and y, where

$$D = (A^2 - 4)C^2 + 4,\ E = C^2 Dx,\ F = 4(A^2 - 4)E^2 + 1,$$

$$G = 1 + CDF - 2(A + 2)(A - 2)^2 E^2,\ H = C + BF + (2y - 1)CF,$$

$$I = (G^2 - 1)H^2 + 1.$$

If $A \geqslant 2$, for any $Z \in \mathbb{Z}^+$ we may require further that $x, y \geqslant Z$.

Lemma 3. Let $A, B, U, V \in \mathbb{Z}$ with $B > 0$. Then

$$(UV)^{B-1} u_B(A, 1) \equiv \sum_{r=0}^{B-1} U^{2r} V^{2(B-1-r)} \pmod{U^2 - AUV + V^2}.$$

Consequently,

$$(V^2 - 1)V^B u_B(A, 1) \equiv V(V^{2B} - 1) \pmod{V^2 - AV + 1}.$$

This can be proved by induction on B.

The first auxiliary theorem

Theorem 1 (Sun [Sci. China Math. 64(2021)]). Let p be a prime, and let $b \in p\uparrow = \{p^n : n \in \mathbb{N}\}$ and $g \in \mathbb{Z}^+$. Let P, Q, X and Y be integers with $P > Q > 0$ and $X, Y \geqslant b$. Suppose that $Y \mid \binom{PX}{QX}$. Then there are integers $h, k, l, w, x, y \geqslant b$ for which

$$DFI \in \square,\ (U^{2P}V^2-4)K^2+4 \in \square,\ pA-p^2-1 \mid (p^2-1)WC-p(W^2-1),$$

$$bw = p^B \ \text{ and } \ 16g^2(C-KL)^2 < K^2,$$

where

$$L := lY,\ U := PLX,\ V := 4gwY,\ W := bw,$$
$$K := QX+1+k(U^PV-2),\ A := U^Q(V+1),\ B := PX+1,$$
$$C := B+(A-2)h,\ D = (A^2-4)C^2+4,\ E = C^2Dx,$$
$$F = 4(A^2-4)E^2+1,\ G = 1+CDF-2(A+2)(A-2)^2E^2,$$
$$H = C+BF+(2y-1)CF,\ I = (G^2-1)H^2+1.$$

On $u_n(A,1)$ with $n \in \mathbb{Z}$

We extend the sequences $u_n = u_n(A,1)$ and $v_n = v_n(A,1)$ to integer indices by letting

$$u_0 = 0,\ u_1 = 1,\ \text{and } u_{n-1} + u_{n+1} = Au_n \text{ for all } n \in \mathbb{Z},$$

and

$$v_0 = 2,\ v_1 = A,\ \text{and } v_{n-1} + v_{n+1} = Av_n \text{ for all } n \in \mathbb{Z}.$$

It is easy to see that

$$u_{-n}(A,1) = -u_n(A,1) = (-1)^n u_n(-A,1)$$

and $v_{-n}(A,1) = v_n(A,1) = (-1)^n v_n(-A,1)$ for all $n \in \mathbb{Z}$.

Lemma 4. Let $A, X \in \mathbb{Z}$. Then

$$(A^2-4)X^2 + 4 \in \square \iff X = u_m(A,1) \text{ for some } m \in \mathbb{Z}.$$

Two more lemmas

Lemma 5 (Sun [Sci. China Ser. A 35(1992)]). Let $A, B, C \in \mathbb{Z}$ with $1 < |B| < |A|/2 - 1$. Then

$$C = u_B(A, 1) \iff (A - 2 \mid C - B) \wedge \exists x \neq 0 \exists y (DFI \in \square),$$

where

$$D = (A^2 - 4)C^2 + 4,\ E = C^2 Dx,\ F = 4(A^2 - 4)E^2 + 1,$$
$$G = 1 + CDF - 2(A + 2)(A - 2)^2 E^2,\ H = C + BF + (2y - 1)CF,$$
$$I = (G^2 - 1)H^2 + 1.$$

Lemma 6 (Sun [Sci. China Ser. A 35(1992)]). Let B, V and W be integers with $B > 0$ and $|V| > 1$. Then $W = V^B$ if there are $A, C \in \mathbb{Z}$ for which $|A| \geqslant \max\{V^{4B}, W^4\}$, $C = u_B(A, 1)$ and

$$(V^2 - 1)WC \equiv V(W^2 - 1) \pmod{AV - V^2 - 1}.$$

The second auxiliary theorem

Theorem 2 (Sun [Sci. China Math. 64(2021)]. Let p be a prime, and let $b \in \mathbb{N}$ and $g \in \mathbb{Z}^+$. Let P, Q, X and Y be integers with

$$P > Q > 0,\ X \geqslant 3b \text{ and } Y \geqslant \max\{b, p^{4P}\}.$$

Suppose that there are integers h, k, l, w, x, y with $lx \neq 0$ for which

$$DFI \in \square,\ (U^{2P}V^2-4)K^2+4 \in \square,\ pA-p^2-1 \mid (p^2-1)WC-p(W^2-1),$$

and $4(C-KL)^2 < K^2$, where where

$$L := lY,\ U := PLX,\ V := 4gwY,\ W := bw,$$

$$K := QX+1+k(U^PV-2),\ A := U^Q(V+1),\ B := PX+1,$$

$$C := B+(A-2)h,\ D = (A^2-4)C^2+4,\ E = C^2Dx,$$

$$F = 4(A^2-4)E^2+1,\ G = 1+CDF-2(A+2)(A-2)^2E^2,$$

$$H = C+BF+(2y-1)CF,\ I = (G^2-1)H^2+1.$$

Then

$$b \in p\uparrow \quad \text{and} \quad Y \mid \binom{PX}{QX}.$$

The third auxiliary theorem

Theorem 3 (Z.-W. Sun [Sci. China Math. 64(2021)]). Let $\mathcal{A} \subseteq \mathbb{N}$ be a Diophantine set, and let p be a prime. Then, for each $a \in \mathbb{N}$, we have

$$a \in \mathcal{A} \Rightarrow \forall Z > 0 \exists f \geqslant Z \exists g \in [b, \mathcal{C}) \left(b \in \square \wedge b \in p\uparrow \wedge Y \mid \binom{pX}{X} \right),$$

$$\exists f \neq 0 \exists g \in [0, 2\mathcal{C}) \left(b \in \square \wedge b \in p\uparrow \wedge Y \mid \binom{pX}{X} \right) \Rightarrow a \in \mathcal{A},$$

where

$$b := 1 + (p^2 - 1)(ap + 1)f,$$

$\mathcal{C} = p^{\alpha_1 p} b^{\alpha_2}$ for some $\alpha_1, \alpha_2 \in \mathbb{Z}^+$ only depending on $\mathcal{A}$, and X and Y are suitable polynomials in $\mathbb{Z}[a, f, g]$ such that if $a \in \mathbb{N}$, $f \in \mathbb{Z} \setminus \{0\}$, $b \in \square$ and $0 \leqslant g < 2\mathcal{C}$ then

$$p + 1 \mid X, \quad X \geqslant 3b \quad \text{and} \quad Y \geqslant \max\{b, p^{4p}\}.$$

Our Main Theorem

Main Theorem (Sun [Sci. China Math. 64(2021)]). Let $\mathcal{A} \subseteq \mathbb{N}$ be any r.e. set. Then there is a polynomial $P_{\mathcal{A}}(z_0, z_1, \ldots, z_9)$ with integer coefficients such that for any $a \in \mathbb{N}$ we have

$$\exists z_1 \ldots \exists z_8 \exists z_9 \geqslant 0[P_{\mathcal{A}}(a, z_1, \ldots, z_9) = 0] \Longrightarrow a \in \mathcal{A},$$

and

$$a \in \mathcal{A} \Longrightarrow \forall Z > 0 \exists z_1 \geqslant Z \ldots \exists z_9 \geqslant Z[P_{\mathcal{A}}(a, z_1, \ldots, z_9) = 0].$$

Remark. As $a \in \mathcal{A}$ if and only if

$$\exists z_1 \geqslant 0 \ldots \exists z_8 \geqslant 0 \exists z_9 \geqslant 0 \left[\prod_{\varepsilon_1, \ldots, \varepsilon_8 \in \{\pm 1\}} P_{\mathcal{A}}(a, \varepsilon_1 z_1, \ldots, \varepsilon_8 z_8, z_9) = 0 \right],$$

the Main Theorem implies Matiyasevich's 9 unknowns theorem.

The 11 Unknowns Theorem

As $n \geqslant 0$ if and only if $n = x^2 + y^2 + z^2 + z$ for some $x, y, z \in \mathbb{Z}$, the Main Theorem implies the following result.

The 11 Unknowns Theorem (Sun [Sci. China Math. 64(2021)]). For any r.e. set $\mathcal{A} \subseteq \mathbb{N}$, there is a polynomial $Q_{\mathcal{A}}(z_0, \ldots, z_{11}) \in \mathbb{Z}[z_0, \ldots, z_{11}]$ such that for any $a \in \mathbb{N}$ we have

$$a \in \mathcal{A} \iff \exists z_1 \cdots \exists z_{11}[Q_{\mathcal{A}}(a, z_1, \ldots, z_{11}) = 0].$$

Consequently, there is no algorithm to decide for any $P(z_1, \ldots, z_{11}) \in \mathbb{Z}[z_1, \ldots, z_{11}]$ whether the equation

$$P(z_1, \ldots, z_{11}) = 0$$

has integer solutions.

Actually we even could require $\deg P < 8.1142 \times 10^{46}$. We view the Main Theorem of the speaker as the `strong form` of the 11 unknowns theorem.

Another Theorem

Theorem (Sun [Sci. China Math. 64(2021)]). Let $\mathcal{A} \subseteq \mathbb{N}$ be any r.e. set. There is a polynomial $Q_{\mathcal{A}}(z_0, z_1, \ldots, z_{10})$ with integer coefficients such that for any $a \in \mathbb{N}$ we have

$$a \in \mathcal{A} \iff \exists z_1 \ldots \exists z_9 \exists z_{10} \neq 0[Q_{\mathcal{A}}(a, z_1, \ldots, z_{10}) = 0].$$

Remark. We can prove this by modifying our proof of the 11 unknowns theorem slightly. This result also implies the 11 unknowns theorem since $z \neq 0 \iff \exists x \exists y(z = (2x + 1)(3y + 1))$.

$P(z_1^2, \ldots, z_{17}^2) = 0$

Theorem (Sun [Sci. China Math. 64(2021)]). Let $\mathcal{A}$ be any r.e. subset of $\mathbb{N}$. Then there is a polynomial $P_4(z_0, z_1, \ldots, z_{17})$ with integer coefficients such that for any $a \in \mathbb{N}$ we have

$$a \in \mathcal{A} \iff \exists z_1 \in \square \ldots \exists z_{17} \in \square[P_4(a, z_1, \ldots, z_{17}) = 0].$$

Remark. To obtain this result we need to modify the proof of the 11 unknowns theorem and make use of

$$\{2^\delta(x^2 - y^2) : \ \delta \in \{0, 1\}, \ x, y \in \mathbb{Z}\} = \mathbb{Z}.$$

Note that $z = (\frac{z+1}{2})^2 - (\frac{z-1}{2})^2$.

Corollary. There is no algorithm to decide for any $P(x_1, \ldots, x_{17}) \in \mathbb{Z}[x_1, \ldots, x_{17}]$ whether the equation

$$P(z_1^2, \ldots, z_{17}^2) = 0$$

has integer solutions.

Part III. Other Developments Related to HTP

Skolem's way to reduce Diophantine equations to one of degree 4

T. A. Skolem (1920s): Any polynomial Diophantine equation over $\mathbb{N}$ or $\mathbb{Z}$ is equivalent to one of degree four.

We illustrate the proof by looking at a particular example. The equation $x^3 + y^5 = z^2 + 4x - 5$ is equivalent to a system of equations of degree two:

$$xu + yv = z^2 + 4x - 5,\ u = x^2,\ v = yw,\ w = yt,\ t = y^2$$

and hence $x^3 + y^5 = z^2 + 4x - 5$ has solutions over $\mathbb{N}$ (or over $\mathbb{Z}$) if and only if the equation

$$(xu+yv-z^2-4x+5)^2+(u-x^2)^2+(v-yw)^2+(w-yt)^2+(t-y^2)^2 = 0$$

has solutions over $\mathbb{N}$ (or over $\mathbb{Z}$).

An equation $P(x_1, \ldots, x_n) = 0$ of degree two is equivalent to the equation $P(x_1, \ldots, x_n)^2 = 0$ of degree four.

Diophantine equations of degree not exceeding four

Combining Skolem's observation with Matiyasevich's theorem, we have

Theorem. There is *no* algorithm to determine whether an arbitrary Diophantine equation of degree 4 has solutions over $\mathbb{N}$ (or over $\mathbb{Z}$).

C. L. Siegel (1972): There is an algorithm to decide whether an arbitrary quadratic Diophantine equation has solutions over $\mathbb{N}$ (or over $\mathbb{Z}$).

Open Question: Does the solvability of an arbitrary cubic Diophantine equation over $\mathbb{N}$ (or over $\mathbb{Z}$) decidable?

HTP for rings of algebraic number fields

Let K be an algebraic number field and O_K be the ring of algebraic integers in K. It is widely believed that Hilbert's Tenth Problem (HTP) over the ring O_K is also undecidable. There are some partial results in this direction.

J. Denef [Proc. Amer. Math. Soc. 1975]: If K is a quadratic number field, then $\mathbb{Z}$ is Diophantine over O_K and hence HTP over O_K is undecidable.

H. N. Shapiro and A. Shlapentokh [Comm. Pure Appl. Math. 1989]: If K is an abelian number fields (i.e., the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian), then $\mathbb{Z}$ is Diophantine over O_K and hence HTP over O_K is undecidable.

M. R. Murty and H. Pasten [J. Number Theory 2017]: Under the Birch and Swinnerton-Dyer conjecture and the automorphy conjecture for L-functions of elliptic curves, HTP over O_K is undecidable for any algebraic number field K.

HTP over $\mathbb{Z}[i]$

Gaussian ring: $\mathbb{Z}[i] = \{a + bi : \ a, b \in \mathbb{Z}\}$.

Lemma (J. Denef [Proc. AMS 48(1975)]). If $x, y \in \mathbb{Z}[i]$ and $x^2 - 4xy + y^2 = 1$, then $x, y \in \mathbb{Z}$.

Auxiliary Theorem (Matiyasevich and Sun, 2019). A number $z \in \mathbb{Z}[i]$ is a rational integer if and only if there are $v, w, x, y \in \mathbb{Z}[i]$ with $v \neq 0$ such that

$$(4(2v(2(2z+1)^2+1) - y)^2 - 3y^2 - 1)^2 + 2(w^2 - 1 - 3y^2(2z + 1 - xy)^2)^2 = 0.$$

Combining this result with the undecidability of $\exists z_1 \cdots \exists z_9 \exists z_{10} \neq 0[P(z_1, \ldots, z_{10}) = 0]$, we obtain the following result.

Theorem (Matiyasevich and Sun, 2019). There is no algorithm to decide whether an arbitrarily given polynomial equation $P(z_1, \ldots, z_{52}) = 0$ (with integer coefficients) over $\mathbb{Z}[i]$ is solvable.

Conjectures

Conjecture 1 (Sun [Sci. China Math. 64(2021)]). There is no algorithm to decide for any $P(x, y, z) \in \mathbb{Z}[x, y, z]$ whether the equation

$$P(x^2, y^2, z^2) = 0$$

has integer solutions.

Remark. This implies that $\exists^3$ over $\mathbb{Z}$ is undecidable as believed by A. Baker, Yu. Matiyasevich and J. Robinson.

Conjecture 2 (Sun, arXiv:2103.08302). $\forall^2\exists^2$ over $\mathbb{Z}$ is undecidable. In other words, there is no algorithm to decide for any $P(x_1, \ldots, x_4) \in \mathbb{Z}[x_1, \ldots, x_4]$ whether for any $a, b \in \mathbb{Z}$ the equation

$$P(a, b, x, y) = 0$$

has solutions with $x, y \in \mathbb{Z}$.

Remark. In contrast, the speaker has proved that $\forall^{10}\exists^2$ and $\forall^2\exists^4$ over $\mathbb{Z}$ are undecidable.

HTP over the rational field $\mathbb{Q}$

It is not known that whether HTP over $\mathbb{Q}$ is decidable or not. If $\mathbb{Z}$ is Diophantine over $\mathbb{Q}$, then HTP over $\mathbb{Q}$ is undecidable since HTP over $\mathbb{Z}$ isundecidable.

Up to now, nobody can show that $\mathbb{Z}$ is Diophantine over $\mathbb{Q}$.

J. Robinson [J. Symbolic Logic 14 (1949)]: $\mathbb{Z}$ is first-order definable over $\mathbb{Q}$ and so the theory $(\mathbb{Q}, +, \cdot)$ is undecidable. Moreover, there is a polynomial

$$F \in \mathbb{Z}[t, x_1, x_2, y_1, \ldots, y_7, z_1, \ldots, z_6]$$

such that $t \in \mathbb{Q}$ is an integer if and only if

$$\forall a \forall b \exists y_1 \ldots \exists y_7 \forall z_1 \ldots \forall z_6 [F(t, a, b, y_1, \ldots, y_7, z_1, \ldots, z_6) = 0]$$

holds over $\mathbb{Q}$. The polynomial F involves

$$M_{a,b} = \{r \in \mathbb{Q} : \ \exists x \exists y \exists z [x^2 + ay^2 - bz^2 = 2 + abr^2]\}.$$

Comments on J. Robinson's work

Hasse-Minkowski Theorem. An integral quadratic form $f(x_1, \ldots, x_n)$ represents 0 in $\mathbb{Q}$ (with $x_1, \ldots, x_n$ not all zero) if and only if f represents 0 in $\mathbb{Q}_\infty = \mathbb{R}$ and in $\mathbb{Q}_p$ for each prime p.

This plays an important role in J. Robinson's way defining $\mathbb{Z}$ in $\mathbb{Q}$.

Comments from R. M. Robinson (J. Robinson's husband):

"She looked at a lot of things that were not helpful. It was several months before she found the Hasse paper. Then she had to find suitable forms to eliminate the various primes from the denominators. Note that it is only the fact that ternary forms represent most numbers with a few exceptions that makes the definition possible. ..... The proof would have been a lot easier for someone who already knew about Hasse's work. But I guess that those who knew it had never heard of Tarski's problem. **It must often happen that the tools for solving a problem are known, but not to the people working on the problem.**"

Further improvements of Robinson's result

B. Poonen [Amer. J. Math. 131 (2009)]: There is a polynomial $G \in \mathbb{Z}[t, x_1, x_2, y_1, \ldots, y_7]$ such that a rational number t is an integer if and only if

$$\forall x_1 \forall x_2 \exists y_1 \ldots \exists y_7 [G(t, x_1, x_2, y_1, \ldots, y_7) = 0]$$

holds over $\mathbb{Q}$.

J. Koenigsmann [Annals of Math. 183 (2016)]: There is a polynomial $H \in \mathbb{Z}[t, x_1, x_2, \ldots, x_n]$ such that a rational number t is *not* an integer, if and only if

$$\exists x_1 \exists x_2 \ldots \exists x_n [H(t, x_1, x_2, \ldots, x_n) = 0]$$

Thus $\mathbb{Q} \setminus \mathbb{Z}$ is Diophantine over $\mathbb{Q}$. (n can be taken as 418.)

N. Daans (2018-2021): For Koenigsmann's theorem, we may take $n = 146,\ 50,\ 38$. To get $n = 38$, Daans needs his joint work with P. Dittmann and A. Fehm [arXiv:2102.06941] via model theory.

Daans' simplification of Koenigsmann's work

Let $\mathbb{P}$ be the set of all primes. For $p \in \mathbb{P}$ let $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers. For $t \in \mathbb{Q}$, clearly

$$t \in \mathbb{Q} \setminus \mathbb{Z} \iff t \neq 0 \wedge t^{-1} \in \bigcup_{p \in \mathbb{P}} p\mathbb{Z}_{(p)}.$$

Let $a, b \in \mathbb{Q}^*$. B. Poonen [Amer. J. Math. 2009] defined

$$S_{a,b} = \{2x_1 \in \mathbb{Q} : \ \exists x_2 \exists x_3 \exists x_4 [x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1]\}$$

and $T_{a,b} = S_{a,b} + S_{a,b} = \{x + y : \ x, y \in S_{a,b}\}$.
For $S, T \subseteq \mathbb{Q}$ we define $T^\times = \{t \in T \setminus \{0\} : \ t^{-1} \in T\}$ and $ST = \{st : \ s \in S \ \& \ t \in T\}$. Daans [arXiv:1812.04372] proved that

$$\bigcup_{p \in \mathbb{P}} p\mathbb{Z}_{(p)} = 2\mathbb{Z}_{(2)} \cup \bigcup_{(a,b) \in \Phi} (J_{a,b}^a \cap J_{a,b}^{2b}),$$

where $\Phi = \{(1 + 4u^2, 2v) : \ u, v \in \mathbb{Z}_{(2)}^\times\}$, and

$$J_{a,b}^c = T_{a,b}\{cy^2 : \ y \in \mathbb{Q} \ \& \ 1 - cy^2 \in \square T_{a,b}^\times\}$$

with $\square = \{r^2 : \ r \in \mathbb{Q}\}$. Also, $\mathbb{Z}_{(2)} = S_{3,3} + S_{2,5}$.

My joint work with Geng-Rui Zhang

Theorem (Geng-Rui Zhang and Z.-W. Sun, arXiv:2104.02520). $\mathbb{Q}\setminus\mathbb{Z}$ has a diophantine representation over $\mathbb{Q}$ with 32 unknowns, i.e., there is a polynomial $P(t,x_1,\ldots,x_{32})\in\mathbb{Z}[t,x_1,\ldots,x_{32}]$ such that for any $t\in\mathbb{Q}$ we have

$$t\notin\mathbb{Z}\iff\exists x_1\cdots\exists x_{32}[P(t,x_1,\ldots,x_{32})=0].$$

Furthermore, the polynomial P can be constructed explicitly with $\deg P<2.1\times10^{11}$.

To obtain this theorem, we start from Daans' work in 2018, and mainly use a new relation-combining theorem on diophantine representations over $\mathbb{Q}$ (which is an analogue of Matiyasevich and Robinson's Relation-Combining Theorem) as an auxiliary tool.

Lemma (Besicovich, 1940). Let K be a field with $\mathrm{ch}(K)\neq2$. For any $a_1,\ldots,a_n\in K$ with $\prod_{s\in I}a_s\notin\{x^2:\ x\in K\}$ for all $\emptyset\neq I\subseteq\{1,\ldots,n\}$, we have $[K(b_1,\ldots,b_n):K]=2^n$, where $b_1,\ldots,b_n$ are elements of $\bar{K}$ with $b_s^2=a_s$ for all $s=1,\ldots,n$.

Relation-Combining Theorem over $\mathbb{Q}$

Relation-Combining Theorem over $\mathbb{Q}$ (G.-R. Zhang and Z.-W. Sun, arXiv:2104.02520). Let $A_1, \ldots, A_k \in \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, and define

$$\mathcal{J}_k(A_1, \ldots, A_k, x) = \prod_{s=1}^{k} A_s^{(k-1)2^{k+1}} \times \prod_{\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}} \left(x + \sum_{s=1}^{k} \varepsilon_s \sqrt{A_s}\, W^{s-1} \right),$$

where

$$W = \left(k + \sum_{s=1}^{k} A_s^2 \right) \left(1 + \sum_{s=1}^{k} A_s^{-2} \right).$$

Then $\mathcal{J}_k(x_1, \ldots, x_k, x)$ is a polynomial with integer coefficients. Moreover,

$$A_1, \ldots, A_k \in \square \iff \exists x [\mathcal{J}_k(A_1, \ldots, A_k, x) = 0],$$

where $\square = \{r^2 : \ r \in \mathbb{Q}\}$.

We use induction on k and make use of Galois theory.

Two lemmas

Any nonnegative rational number can be written as $a/b = (ab)/b^2$ with $a, b \in \mathbb{N}$ and $b > 0$. So Lagrange's four-square theorem yields the following lemma.

Lemma. Let $r \in \mathbb{Q}$. Then

$$r \geqslant 0 \iff \exists w \exists x \exists y \exists z [r = w^2 + x^2 + y^2 + z^2].$$

We also make use of the following useful lemma.

Robinson's Lemma (cf. D. Flath and S. Wagon [Amer. Math. Monthly 98(1991)]). Let r be any rational number. Then

$$r \in \mathbb{Z}_2 \iff \exists x \exists y \exists z [7r^2 + 2 = x^2 + y^2 + z^2].$$

This can be proved directly by using the Gauss-Legendre theorem

$$\mathbb{N} \setminus \{x^2 + y^2 + z^2 : \ x, y, z \in \mathbb{Z}\} = \{4^k(8m + 7) : \ k, m \in \mathbb{N}\}.$$

$\forall^9\exists^{32}$ over $\mathbb{Q}$ is undecidable

Combining the speaker's strong form of the 11 unknowns theorem with Zhang and Sun's result that $\mathbb{Q} \setminus \mathbb{Z}$ is diophantine over $\mathbb{Q}$ with 32 unknowns, we obtain the following result.

Theorem (G.-R. Zhang and Z.-W. Sun, arXiv:2104.02520). $\forall^9\exists^{32}$ over $\mathbb{Q}$ is undecidable, i.e., there is no algorithm to determine for any $P(x_1, \ldots, x_{41}) \in \mathbb{Z}[x_1, \ldots, x_{41}]$ whether

$$\forall x_1 \cdots \forall x_9 \exists y_1 \cdots \exists y_{32}[P(x_1, \ldots, x_9, y_1, \ldots, y_{32}) = 0],$$

where variables range over $\mathbb{Q}$.

Proof. For any $x \in \mathbb{Q}$, we clearly have

$$\begin{aligned} x < 0 &\iff x \neq 0 \wedge -x \geqslant 0 \\ &\iff \exists y_1(xy_1 = 1) \wedge \exists y_1 \exists y_3 \exists y_4 \exists y_5(-x = y_2^2 + y_3^2 + y_4^2 + y_5^2) \\ &\iff \exists y_1 \cdots \exists y_5[(xy_1 - 1)^2 + (x + y_2^2 + y_3^2 + y_4^2 + y_5^2)^2 = 0]. \end{aligned}$$

Proof of the undecidability of $\forall^9\exists^{32}$ over $\mathbb{Q}$

As proved by Zhang and Sun, there is a polynomial $f(y_1, \ldots, y_{32}) \in \mathbb{Z}[y_1, \ldots, y_{32}]$ such that for any $x \in \mathbb{Q}$ we have

$$x \notin \mathbb{Z} \iff \exists y_1 \cdots \exists y_{32}[f(y, y_1, \ldots, y_{32}) = 0].$$

Let $P(x_1, \ldots, x_9) \in \mathbb{Z}[x_1, \ldots, x_9]$. Then

$$\begin{aligned}
&\neg\exists x_1 \in \mathbb{Z} \cdots \exists x_8 \in \mathbb{Z} \exists x_9 \in \mathbb{N}[P(x_1, \ldots, x_9) = 0] \\
\iff &\forall x_1 \cdots \forall x_9[\neg(x_1, \ldots, x_9 \in \mathbb{Z} \wedge x_9 \geq 0) \vee P(x_1, \ldots, x_9) \neq 0] \\
\iff &\forall x_1 \cdots \forall x_9[\vee_{t=1}^{9}(x_t \notin \mathbb{Z}) \vee x_9 < 0 \vee P(x_1, \ldots, x_9) \neq 0] \\
\iff &\forall x_1 \cdots \forall x_9[\vee_{t=1}^{9} \exists y_1 \cdots \exists y_{32}(f(x_t, y_1, \ldots, y_{32}) = 0) \\
&\vee -x_9 > 0 \vee \exists y_1(y_1 P(x_1, \ldots, x_9) - 1 = 0] \\
\iff &\forall x_1 \cdots \forall x_9 \exists y_1 \cdots \exists y_{32}[P^*(x_1, \ldots, x_9, y_1, \ldots, y_{32}) = 0],
\end{aligned}$$

where $P^*(x_1, \ldots, x_9, y_1, \ldots, y_{32})$ is the polynomial

$$\begin{aligned}
&(y_1 P(x_1, \ldots, x_9) - 1) \prod_{t=1}^{9} f(x_t, y_1, \ldots, y_{32}) \\
&\times \left((x_9 y_1 - 1)^2 + (x_9 + y_2^2 + y_3^2 + y_4^2 + y_5^2)^2\right).
\end{aligned}$$

References

For main sources, you may look at:

1. N. Daans, *Universally defining finite generated subrings of global fields*, preprint, arXiv:1812.04372, 2018.

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

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

4. J. Koenigsmann, *Defining* $\mathbb{Z}$ *in* $\mathbb{Q}$, Annals of Math. **183** (2016), 73–93.

5. Y. Matiyasevich and Z.-W. Sun, *On Diophantine equations over* $\mathbb{Z}[i]$ *with* 52 *unknowns*, accepted for publication in Proc. of the 2019 Asian Logic Conf. (World Sci.) (`arXiv:2002.12136`).

References (continued)

6. B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), 675–682.

7. J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.

8. Z.-W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Math. 35(1992), 257–269.

9. Z.-W. Sun, *Further results on Hilbert's Tenth Problem*, Sci. China Math. **64** (2021), 281–306.

10. G.-R. Zhang and Z.-W. Sun, $\mathbb{Q} \setminus \mathbb{Z}$ *is diophantine over* $\mathbb{Q}$ *with* 32 *unknowns*, preprint, arXiv:2104.02520, 2021.

Thank you!