A talk given at Institute of Math., Chinese Academy of Sciences
(Beijing, April 18, 2017)
and the 5th National Conf. of Combin. Number Theory
(Huai'an, Sept. 16, 2017)
and the 2017 Number Theory Days in Hangzhou (Sept. 24, 2017)
and the 16th Asian Logic Conf. (Nur-Sultan, Kazakhstan; June 18, 2019)

Further Results on Hilbert's Tenth Problem

Zhi-Wei Sun

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

Abstract

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

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

(with integer coefficients) has solutions over the ring $\mathbb{Z}$ of the integers. This was finally solved by Matiyasevich in 1970 negatively. In this talk we introduce the speaker's further results on HTP. In particular, we present a sketch of the proof of the speaker's main result that there is no effective algorithm to determine whether an arbitrary polynomial equation $P(x_1, \ldots, x_{11}) = 0$ (with integer coefficients) in 11 unknowns has integral solutions or not.

My logic experience

David Hilbert$\longrightarrow$ Paul Bernays$\longrightarrow$Shawkwei Moh$\longrightarrow$Zhi-Wei Sun

In 1983, I entered Department of Mathematics, Nanjing University. My speciality is *Mathematical Logic*. During 1987-1992, I was a graduate student at Nanjing University.

In 1992, I got my PhD under the supervision of Prof. Shawkwei Moh with the thesis *Further Results on Hilbert's Tenth Problem*.

Since July 1992 I have worked as a teacher at Nanjing University. In 1994 I turned my interest from *Mathematical Logic* to *Number Theory* (especially *Combinatorial Number Theory*).

Part I. Hilbert's Tenth Problem and its Solution

Hilbert's Tenth Problem

In 1900, at the Paris conference of ICM, D. Hilbert presented 23 famous mathematical problems. He formulated his tenth problem as follows:

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 in a finite number of operations whether the equation is solvable in rational integers.

In modern language, Hilbert's Tenth Problem (HTP) asked 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.

Partial recursive functions

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Zero Function: $O(x) = 0$ (for all $x \in \mathbb{N}$).

Successor Function: $S(x) = x + 1$.

Projection Function: $I_{nk}(x_1, \ldots, x_n) = x_k$ $(1 \leqslant k \leqslant n)$

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 natural number y such that $g(x_1, \ldots, x_n, y) = 0$. 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 $O(x), S(x), I_{nk}$ and those obtained from the basic functions by applying composition and μ-operator a finite number of times.

Partial recursive functions coincide with the Turing computable functions via the Turing machine which manipulates symbols on a strip of tape according to a table of rules (i.e., a program).

r.e. sets

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 (or a Turing computable function).

A set $A \subseteq \mathbb{N}$ is said to be *r.e. (recursively enumerable) set* or *semi-computable* if there is a partial recursive function $f(x)$ such that

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

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

There are nonrecursive r.e. subsets of $\mathbb{N}$ such as $K = \{x \in \mathbb{N} : \ \varphi_x(x) \text{ is defined}\}$, where φ_n denotes the n-th partial recursive function of one variable.

A problem or a set is *decidable*, if and only if its characteristic function is Turing computable (or recursive).

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

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

(Throughout this paper, variables always range over $\mathbb{Z}$.)

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 is an r.e. set.

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.

Eliminate bounded universal quantifier

Theorem (M. Davis, H. Putnam and J. Robinson [Annals of Math. 1961]) Let $b \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, $P(y, x_1, \ldots, x_m) \in \mathbb{Z}[y, x_1, \ldots, x_m]$, 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

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

$\Longleftrightarrow$ 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. A system of finitely many Diophantine equations is equivalent to a single Diophantine equation. 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

$$P_1(z_1, \ldots, z_n) = 0 \ \& \ \ldots \ \& \ P_k(z_1, \ldots, z_n) = 0$$

$$\Longleftrightarrow P_1^2(z_1, \ldots, z_n) + \ldots + P_k^2(z_1, \ldots, z_n) = 0.$$

Two key steps to solve HTP

Based on the above theorem, M. Davis, H. Putnam and J. Robinson [Ann. of Math. 1961] successfully showed that any r.e. set is exponential Diophantine, that is, any r.e. set A has the exponential Diophantine representation

$$a \in A \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0[P(a, x_1, \ldots, x_n, 2^{x_1}, \ldots, 2^{x_n}) = 0],$$

where P is a polynomial with integer coefficients.

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

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

increases exponentially. In 1970 Yu. Matiyasevich took the last step to show ingeniously that the relation $y = F_{2x}$ (with $x, y \in \mathbb{N}$) is Diophantine! It follows that the exponential relation $a = b^c$ (with $a, b, c \in \mathbb{N}$, $b > 1$ 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

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

Matjiasevich's theorem

Matiyasevich's surprising result, together with the important work of Davis, Putnam and Robinson in 1961, leads to the following great result.

Matiyasevich's Theorem (1970). Any r.e. set $A \subseteq \mathbb{N}$ is Diophantine.

As some r.e. sets are not recursive, it follows that there is *no* algorithm to decide whether an *arbitrary* polynomial equation

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

(with integer coefficients) has solutions $x_1, \ldots, x_n \in \mathbb{N}$.

The negative solution to HTP

J. Robinson's Simple Observation:

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

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

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

Therefore, the negative solution of HTP (over $\mathbb{Z}$) is equivalent to the negative solution of HTP (over $\mathbb{N}$).

Thus Matiyasevich solved HTP negatively!

Part II. Reduction of Natural Number Unknowns

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])

Matiyasevich-Robinson's Relation-Combining Theorem

Let $\square$ denote the set of all integer squares.

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

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

where $M_k(x_1, \ldots, x_k, w, x, y, z)$ is a polynomial with integer coefficients.

Matiyasevich-Robinson Relation-Combining Theorem is an important tool to reduce the number of unknowns.

Coding idea of Matiyasevich and Robinson (1975)

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

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

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

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

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 $z_0, \ldots, z_\nu \in [0, b]$

$\Longleftrightarrow$ 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 Matiyasevich to 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.

Part III. Find small ν with $\exists^\nu$ over $\mathbb{Z}$ undecidable

$\exists$ 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

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

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.

$\exists^{11}$ 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 adapted 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 (including Davis and Matiyasevich) wanted to see my detailed proof, I did not write an English version of that, since I was busy with new discoveries.

After 25 years had passed, in 2017 I finally wrote an English paper containing the undecidability of $\exists^{11}$ over $\mathbb{Z}$ as well as my new discoveries related to HTP. The preprint is publicly available from `http://arxiv.org/abs/1704.03504`

Lucas sequences

Let A and B be integers. The usual Lucas sequence $u_n = u_n(A, B)$ $(n = 0, 1, 2, \ldots)$ and its companion $v_n = v_n(A, B)$ $(n = 0, 1, 2, \ldots)$ are defined as follows:

$$u_0 = 0,\ u_1 = 1,\ \text{and}\ u_{n+1} = Au_n - Bu_{n-1}\ (n = 1, 2, 3, \ldots);$$

and

$$v_0 = 2,\ v_1 = A,\ \text{and}\ v_{n+1} = Av_n - Bv_{n-1}\ (n = 1, 2, 3, \ldots).$$

Note that

$$u_n(2, 1) = n,\ u_n(1, -1) = F_n,\ \text{and}\ u_n(3, 1) = F_{2n}.$$

Let

$$\alpha = \frac{A + \sqrt{\Delta}}{2} \text{ and } \beta = \frac{A - \sqrt{\Delta}}{2}$$

be the two roots of the quadratic equation $x^2 - Ax + B = 0$ where $\Delta = A^2 - 4B$. It is well known that for any $n \in \mathbb{N}$ we have

$$(\alpha - \beta)u_n = \alpha^n - \beta^n,\ v_n = \alpha^n + \beta^n \text{ and } v_n^2 - \Delta u_n^2 = 4B^n.$$

Pell's equation

Let $d \in \mathbb{Z}^+ \setminus \square$. It is well-known that the Pell equation

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

has infinitely many integral solutions. (Note that $x = 0$ and $y = \pm 1$ are trivial solutions.) Moreover,

$$\{y + \sqrt{d}x : \ x, y \in \mathbb{Z} \text{ and } y^2 - dx^2 = 1\}$$

is a multiplicative cyclic group.

For any integer $A \geqslant 2$, the solutions of the Pell equation

$$y^2 - (A^2 - 1)x^2 = 1 \ \ (x, y \in \mathbb{N})$$

are given by $x = u_n(2A, 1)$ and $y = v_n(2A, 1)$ with $n \in \mathbb{N}$. J. Robinson and his followers wrote $u_n(2A, 1)$ and $v_n(2A, 1)$ as $\psi_n(A)$ and $\chi_n(A)$ respectively.

To unify Matiyasevich's use of $F_{2n} = u_n(3, 1)$ and Robinson's use of $\psi_n(A) = u_n(2A, 1)$, we deal with Lucas sequences $(u_n(A, 1))_{n \geqslant 0}$.

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

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

Remark. For $n \in \mathbb{N}$ and $A \geqslant 2$, it is easy to show that

$$(A-1)^n \leqslant u_{n+1}(A,1) \leqslant A^n.$$

Diophantine representation of $C = u_B(A, 1)$ with unknowns arbitrarily large

Matiyasevi c and Robinson (1975) showed that for $A > 1$ and $B, C > 0$ there is a Diophantine representation of $C = u_B(2A, 1)$ only involving three natural number variables.

Lemma (Sun [Sci. China Ser. A 35(1992)]). Let $A, B, C \in \mathbb{Z}$ with $A > 1$ and $B \geqslant 0$. Then

$$C = u_B(A, 1) \iff C \geqslant B \wedge \exists x > 0 \exists y > 0 (DFI \in \square)$$

$$\iff \exists x, y, z \geqslant 0 [DFI(C - B + 1)^2 = (z - DFI(C - B + 1))^2],$$

where

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

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

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

Moreover, if $C = u_B(A, 1)$ with $B > 0$, then for any $Z \in \mathbb{Z}^+$ there are integers $x \geqslant Z$ and $y \geqslant Z$ with $DFI \in \square$.

Diophantine representation of $C = u_B(A, 1)$ with integer unknowns

Clearly $C \geqslant B \iff \exists x \geqslant 0(C = B + x)$. However, if we use integer variables, we need three variables:

$$C \geqslant B \iff \exists x \exists y \exists z[C = B + x^2 + y^2 + z^2 + z].$$

Thus, **to save the number of integer variables involved, we should try to avoid inequalities**.

Note that

$$u_B(A, 1) \equiv u_B(2, 1) = B \pmod{A - 2}.$$

Lemma (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, F, I are defined as before.

Diophantine representation of $W = V^B$ with integer unknowns

J. Robinson showed that $W = V^B$ (with $V > 1$ and $B, W > 0$) if and only if there is an integer $A > \max\{V^{3B}, W^B\}$ such that

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

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

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

Remark. A, V and W in this lemma are not necessarily positive, they might be negative.

The first auxiliary theorem

Theorem 1 (Sun, arXiv:1704.03504). 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

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

and

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

where

$$p\uparrow := \{p^k : \ k = 0, 1, 2, \ldots\} \ \text{ and } \ b := 1 + (p^2 - 1)(ap + 1)f,$$

$\mathcal{C} = p^{\alpha_1 p} b^{\alpha_2}$ 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 $0 \leq g < 2\mathcal{C}$ then

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

Remark. Clearly, $b \in \square \wedge f \neq 0 \Rightarrow f > 0 \wedge b > a \wedge p^2 - 1 \mid b - 1$.

The second auxiliary theorem

Theorem 2 (Sun, arXiv:1704.03504). Let p be a prime, and let $b \in p\uparrow$ and $g \in \mathbb{Z}^+$. Let P, Q, X, 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

$$L := IY,\ U := PLX,\ V := 4gwY,$$
$$W := bw,\ K := QX+1+k(U^PV-2),$$
$$A := U^Q(V+1),\ B := PX+1,\ C := B+(A-2)h,$$

and D, F, I are as before.

Remark. We actually take $C = u_B(A,1)$, $K = u_{QX+1}(U^PV,1)$, $L = \lfloor (V+1)^{PX}/V^{QX} \rfloor \equiv \binom{PX}{QX} \pmod V$.

The third auxiliary theorem

Theorem 3 (Sun, arXiv:1704.03504). Let p be a prime, and let $b \in \mathbb{N}$ and $g \in \mathbb{Z}^+$. Let P, Q, X, 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 $lx \neq 0$ such that

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

and

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

where we adopt previous notations. Then

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

Remark. This theorem involving integer variables plays a central role in our proof of the undecidability of $\exists^{11}$ over $\mathbb{Z}$.

Main Theorem

Theorem (Sun, arXiv:1704.03504). Let $\mathcal{A} \subseteq \mathbb{N}$ be an r.e. set.

(i) 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

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

(ii) 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

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

Two Lemmas

Lemma 1. For any $A_1, \ldots, A_k, S, T \in \mathbb{Z}$ with $S \neq 0$, we have

$$A_1 \in \square \wedge \cdots \wedge A_k \in \square \wedge S \mid T \iff \exists z[H_k(A_1, \ldots, A_k, S, T, z) = 0],$$

where H_k is a suitable polynomial with integer coefficients.

Remark. This is motivated by Matiyasevich-Robinson's Relation-Combining Theorem. Note that z is an integer variable.

Lemma 2 (Sun, arXiv:1704.03504). Let $m \in \mathbb{Z}$. Then

$$m \geqslant 0 \iff \exists x \neq 0[(3m-1)x^2 + 1 \in \square].$$

Remark. This is easy since if $m \in \mathbb{Z}^+$ then $3m - 1 \notin \square$ and hence the Pell equation

$$y^2 - (3m-1)x^2 = 1$$

has infinitely many integral solutions.

A corollary

As some r.e. sets are not Diophantine, the Main Theorem has the following consequence.

Corollary. (i) There is no algorithm to determine for any $P(z_1, \ldots, z_9) \in \mathbb{Z}[z_1, \ldots, z_9]$ whether the equation

$$P(z_0, \ldots, z_9) = 0$$

has integral solutions with $z_9 \geqslant 0$ (or $z_1 + \ldots + z_9 \geqslant 0$).

(ii) There is no algorithm to determine for any $Q(z_1, \ldots, z_{10}) \in \mathbb{Z}[z_1, \ldots, z_9]$ whether the equation

$$Q(z_0, \ldots, z_{10}) = 0$$

has integral solutions with $z_{10} \neq 0$ (or $z_1 + \ldots + z_{10} \neq 0$).

Remark. Let $z_9' = z_9 - z_1 - \ldots - z_8$. Then

$$P(z_1, \ldots, z_8, z_9') = 0 \text{ with } z_1 + \ldots + z_8 + z_9' \geqslant 0$$
$$\iff P(z_1, \ldots, z_8, z_9) = 0 \text{ with } z_9 \geqslant 0.$$

$\exists^{11}$ over $\mathbb{Z}$ is undecidable

Recall that

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

So,

$$\begin{aligned} &\exists z_1 \ldots \exists z_8 \exists z_9 \geqslant 0 [P(z_1, \ldots, z_8, z_9) = 0] \\ \iff &\exists z_1 \ldots \exists z_{11} [P(z_1, \ldots, z_8, z_9^2 + z_{10}^2 + z_{11}^2 + z_{11}) = 0]. \end{aligned}$$

Similarly, in view of S. P. Tung's observation (1985)

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

we have

$$\begin{aligned} &\exists z_1 \ldots \exists z_9 \exists z_{10} \neq 0 [Q(z_1, \ldots, z_9, z_{10}) = 0] \\ \iff &\exists z_1 \ldots \exists z_{11} [Q(z_1, \ldots, z_9, (2z_{10} + 1)(3z_{11} + 1)) = 0]. \end{aligned}$$

Therefore, both parts of the Main Theorem implies the undecidability of $\exists^{11}$ over $\mathbb{Z}$.

Quantifier prefixes over Diophantine equations

In 1987 S.P. Tung proved for each $n \in \mathbb{Z}^+$ that $\forall^n\exists$ over $\mathbb{Z}$ is co-NP-complete. He also showed that $\forall^{27}\exists^2$ over $\mathbb{Z}$ is undecidable, and asked whether 27 here can be replaced by a smaller number. Corollary 2 of us tells that $\forall^{10}\exists^2$ over $\mathbb{Z}$ and $\forall^9\exists^3$ over $\mathbb{Z}$ are undecidable.

In 1975 Matiyasevich and Robinson showed that $\exists^2\forall\exists$ with $\forall$ bounded is undecidable over $\mathbb{N}$. In 1981 Jones obtained the decidability of $\forall\exists$ over $\mathbb{N}$ as well as some other undecidable results over $\mathbb{N}$.

In my PhD thesis in 1992, I also proved that

$$\forall\exists^6,\ \forall^2\exists^4,\ \forall\exists\forall\exists^3,\ \forall\exists\forall^3\exists^2,\ \forall^2\exists\forall^2\exists^2,\ \forall\exists^2\forall^2\exists^2,$$
$$\exists^2\forall\exists^3,\ \exists^2\forall^3\exists^2,\ \exists\forall\exists\forall^2\exists^2,\ \exists\forall\exists^4,\ \exists\forall^2\exists^3,\ \exists\forall^5\exists^2$$

over $\mathbb{Z}$ are undecidable, and that

$$\exists^2\forall\exists^3,\ \exists^2\forall^2\exists^2,\ \exists\forall\exists\forall\exists^2,\ \exists\forall\exists^4,\ \exists\forall^2\exists^3,\ \exists\forall^4\exists^2$$

with $\forall$ bounded by polynomials are undecidable over $\mathbb{Z}$.

Part IV. Undecidable results related to polygonal numbers

Polygonal numbers

Recall that triangular numbers have the form $T_x = x(x+1)/2$ with $x \in \mathbb{Z}$. Note that $T_{-1-x} = T_x$.

Polygonal numbers are nonnegative integers constructed geometrically from the regular polygons. For $m = 3, 4, 5, \ldots$, the m-gonal numbers are given by

$$p_m(n) = (m-2)\binom{n}{2} + n \quad (n = 0, 1, 2, \ldots).$$

Clearly

$$p_3(n) = T_n,\ p_4(n) = n^2,\ p_5(n) = \frac{3n^2 - n}{2},\ p_6(n) = 2n^2 - n = T_{2n-1}.$$

The larger m is, the more sparse m-gonal numbers are.

Fermat claimed that for each $m = 3, 4, \ldots$ any $n \in \mathbb{N}$ can be written as the sum of m polygonal numbers of order m. This was proved by Lagrange for $m = 4$, Gauss for $m = 3$, and Cauchy for $m \geqslant 5$.

Generalized pentagonal numbers and octagonal numbers

For $m = 5, 6, \ldots$ those $p_m(x)$ with $x \in \mathbb{Z}$ are called *generalized polygonal numbers of order m*. We set

$$\mathrm{Tri} = \{T_x : \ x \in \mathbb{Z}\}, \ \mathrm{Pen} = \left\{p_5(x) = \frac{x(3x-1)}{2} : \ x \in \mathbb{Z}\right\}$$

and

$$\mathrm{Octa} = \{p_8(x) = x(3x-2) : \ x \in \mathbb{Z}\}.$$

R. K. Guy [Amer. Math. Monthly 101(1994)]: Each $n \in \mathbb{N}$ is the sum of three elements of Pen.

Z.-W. Sun [J. Number Theory, 162(2016)]: Any $n \in \mathbb{N}$ is the sum of four elements of Octa. (This is quite similar to Lagrange's four-square theorem.)

Clearly,

$$x = \frac{x(x+1)}{2} - \frac{x(x-1)}{2} = T_x - T_{-x},$$

$$x = \frac{x(3x+1)}{2} - \frac{x(3x-1)}{2} = p_5(-x) - p_5(x).$$

A lemma on squares and generalized octagonal numbers

Lemma (Sun, arXiv:1704.03504). (i) Any integer can be written as $2^\delta(x^2-y^2)$ with $\delta\in\{0,1\}$ and $x,y\in\mathbb{Z}$. Also, each integer can be written as $2^\delta(p_8(x)-p_8(y))$ with $\delta\in\{0,1\}$ and $x,y\in\mathbb{Z}$.

(ii) Any positive odd integer can be written as $x^2+y^2+2z^2$ with $x,y,z\in\mathbb{Z}$. Also, each positive odd integer can be written as $p_8(x)+p_8(y)+2p_8(z)$ with $x,y,z\in\mathbb{Z}$.

The first assertion in part (ii) is known.

Let $n\in\mathbb{Z}^+$. By Lemma 4.3(ii) of Sun [J. Number Theory, 162(2016)], $6n+1=x^2+y^2+2z^2$ for some $x,y,z\in\mathbb{Z}$ with $3\nmid xyz$. (This is a nontrivial result!) Without loss of generality we may assume that $x=3u-1$, $y=3v-1$ and $z=3w-1$ for some $u,v,w\in\mathbb{Z}$. Thus

$$\begin{aligned}6n+1=&(3u-1)^2+(3v-1)^2+2(3w-1)^2\\=&(3p_8(u)+1)+(3p_8(v)+1)+2(3p_8(w)+1)\end{aligned}$$

and hence $2n-1=p_8(u)+p_8(v)+2p_8(w)$.

Undecidable results related to Tri, □, Pen and Octa

Theorem (Z. W. Sun, arXiv:1704.03504). 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

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

Also, there are polynomials

$$P_3(z_0, z_1, \ldots, z_{18}),\ P_5(z_0, z_1, \ldots, z_{18}),\ P_8(z_0, z_1, \ldots, z_{18})$$

with integer coefficients such that for any $a \in \mathbb{N}$ we have

$$\begin{aligned} a \in \mathcal{A} &\iff \exists z_1 \in \mathrm{Tri} \ldots \exists z_{18} \in \mathrm{Tri}[P_3(a, z_1, \ldots, z_{18}) = 0] \\ &\iff \exists z_1 \in \mathrm{Pen} \ldots \exists z_{18} \in \mathrm{Pen}[P_5(a, z_1, \ldots, z_{18}) = 0] \\ &\iff \exists z_1 \in \mathrm{Octa} \ldots \exists z_{18} \in \mathrm{Octa}[P_8(a, z_1, \ldots, z_{18}) = 0], \end{aligned}$$

Corollary. $\exists^{17}$ over $\square$, $\exists^{18}$ over Tri, $\exists^{18}$ over Pen, and $\exists^{18}$ over Octa are all undecidable.

On the set of primes

Let $\mathcal{P}$ be the set of all (positive) primes.

Matiyasevich (1975). There is a polynomial $P(x_1,\ldots,x_{10})\in\mathbb{Z}[x_1,\ldots,x_{10}]$ such that

$$\mathcal{P}=\mathbb{N}\cap\{P(x_1,\ldots,x_{10}):\ x_1,\ldots,x_{10}\in\mathbb{N}\}.$$

Theorem (Sun, arXiv:1704.03504). There are polynomials $\hat{P}(z_1,\ldots,z_{20})$, $\tilde{P}(z_1,\ldots,z_{21})$ with integer coefficients such that

$$\begin{aligned}\mathcal{P}=&\mathbb{N}\cap\{\hat{P}(z_1^2,\ldots,z_{20}^2):\ z_1,\ldots,z_{20}\in\mathbb{N}\}\\ =&\mathbb{N}\cap\{\tilde{P}(z_1(3z_1+2),\ldots,z_{21}(3z_{21}+2)):\ z_1,\ldots,z_{21}\in\mathbb{N}\}.\end{aligned}$$

In the proof we need the Putnam trick (1969): For any polynomial $P(x)\in\mathbb{Z}[x]$, we have

$$\mathbb{N}\cap\{(x+1)(1-P(x)^2)-1:\ x\in\mathbb{N}\}=\{x\in\mathbb{N}:\ P(x)=0\}.$$

We also use the observation that any prime has the form $x^2+y^2+2z^2$ (or $p_8(x)+p_8(y)+2p_8(z)$) with $x,y,z\in\mathbb{Z}$.

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 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 a rational number t is an integer if and only if

$$\forall x_1 \forall x_2 \exists y_1 \ldots \exists y_7 \forall z_1 \ldots \forall z_6 [F(t, x_1, x_2, y_1, \ldots, y_7, z_1, \ldots, z_6) = 0]$$

holds over $\mathbb{Q}$.

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 an integer, if and only if

$$\forall x_1 \forall x_2 \ldots \forall x_n [H(t, x_1, x_2, \ldots, x_n) \neq 0]$$

holds over $\mathbb{Q}$, i.e., the equation

$$H(t, x_1, \ldots, x_n) = 0$$

has no solutions with $x_1, \ldots, x_n \in \mathbb{Q}$. Thus $\mathbb{Q} \setminus \mathbb{Z}$ is Diophantine over $\mathbb{Q}$.

References

For main sources of my work mentioned here, you may look at:

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

2. Z.-W. Sun, *A new relation-combining theorem and its application*, Z. Math. Logik Grundlag. Math. 38(1992), 209-212.

3. Z.-W. Sun, *Further results on Hilbert's tenth problem*, arXiv:1704.03504, http://arxiv.org/abs/1704.03504.

Thank you!