A plenary talk given at the 2021 Chinese Annual Conf. on Math. Logic (Tianjin, July 9-11, 2021)

The 11 Unknowns Theorem and its Applications

Zhi-Wei Sun

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

July 10, 2021

Abstract

We first review the history of Hilbert's Tenth Problem as well as the speaker's 11 unknowns theorem which states that there is no algorithm to decide for any $P(x_1, \ldots, x_{11}) \in \mathbb{Z}[x_1, \ldots, x_{11}]$ whether the equation $P(x_1, \ldots, x_{11}) = 0$ has integer solutions.

We then talk about some applications of the 11 unknowns theorem. In particular, the 11 unknowns theorem can be used to deduce that there is no algorithm to decide for any $P(z_1, \ldots, z_{52}) \in \mathbb{Z}[z_1, \ldots, z_{52}]$ whether the equation $P(z_1, \ldots, z_{52}) = 0$ has solutions over the Gaussian ring $\mathbb{Z}[i]$.

Finally we introduce the speaker's recent result with Geng-Rui Zhang which states that $\mathbb{Q} \setminus \mathbb{Z}$ is diophantine over $\mathbb{Q}$ with 32 unknowns. Combining this with the strong version of the 11 unknowns theorem, we obtain that there is no algorithm to decide for any polynomial $P(x_1, \ldots, x_9, y_1, \ldots, y_{32})$ with integer coefficients 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 $\mathbb{Q}$.

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

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

Recursively enumerable sets and recursive sets

A subset A of $\mathbb{N} = \{0, 1, \ldots\}$ 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 (equivalently, Turing computable function).

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. It is known that there are r.e. sets which are not recursive.

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.

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

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

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.

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 (as conjectured by M. Davis). 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's 9 unknowns theorem**, 1975; details in Jones [J. Symbolic Logic, 1982])

Matiyasevich-Robinson Relation-Combining Theorem

Matiyasevich and Robinson [Acta Arith. 27(1975)] introduced

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

with $X = 1+\sum_{i=1}^{k} x_i^2$. They showed that this polynomial has integer coefficients and that $A_1,\ldots,A_k \in \mathbb{Z}$ are all squares if and only if $J_k(A_1,\ldots,A_k,x) = 0$ for some $x \in \mathbb{Z}$.

Matiyasevich-Robinson Relation-Combining Theorem. Let $A_1,\ldots,A_k,R,S$ and 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 $\square = \{x^2 : \ x \in \mathbb{Z}\}$, and $M_k(x_1,\ldots,x_k,w,x,y,z)$ is

$$(w^2(1-2y))^{2^k} J_k\left(x_1,\ldots,x_k,x^2+X^k+\frac{x^2+w^2z}{w^2(1-2y)}\right)$$

with $X = 1+\sum_{j=1}^{k} x_j^2$.

(For the $\Rightarrow$ direction we may even require $n \geqslant 1+\sum_{j=1}^{k} A_j^2$.)

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 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 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,

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

Remark. This can be proved by induction on B, and a weaker version is due to J. Robinson.

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

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

A lemma involving Pell's equation

Lemma 7 (Sun [Sci. China Math. 64(2021)] Let $m \in \mathbb{Z}$. Then

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

Proof. Clearly, $(3 \times 0 - 1)1^2 + 1 \in \square$.

If $m < 0$ and $x \in \mathbb{Z} \setminus \{0\}$, then $(3m-1)x^2 + 1 \leqslant -4 + 1 < 0$.

If $m > 0$, then $3m - 1 > 0$ and $3m - 1 \notin \square$, hence the Pell equation $y^2 - (3m-1)x^2 = 1$ has infinitely many integral solutions and thus $(3m-1)x^2 + 1 \in \square$ for some nonzero integer x.

In view of the above, we have completed the proof.

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. Applications of the 11 unknowns theorem

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.

Application of the 11 unknowns theorem to dynamic geometry

In 2002, J. Richter-Gebert and U. Kortenkamp applied the 11 unknowns theorem to obtain a undecidable result in dynamic geometry.

Theorem. Let P be a GSP over the JMBW instruction set with at least 11 WHEEL-operations and two BISECT-operations. Let A and B be two admissible instances of P. It is undecidable whether there is an admissible real path from A to B.

GSP–Geometric Straight Line Program with four basic points $(0,0),(1,0),(0,1),(1,1)$.

J–Join. Draw a line passing two distinct points.

M–Meet. Find the intersection point of two lines.

B–Bisect. Draw the angular bisector of two lines passing through the origin O.

W–Wheel. Find an angle θ for a point $P=(x,y)\neq(0,0)$ with $x+yi=re^{2\pi i\theta}$ for some $r>0$.

Application of the 11 unknowns theorem to the fixed point problem of the SRL language

The programming language SRL has distinctive features:

(i) Every program that mentions n registers defines a bijection from $\mathbb{Z}^n$ to $\mathbb{Z}^n$.

(ii) The generation of the SRL-program that computes the inverse of the bijection can be automatic.

In 2020 A.B. Matos, L. Paolini and L. Roversi [Theoret. Comput. Sci. 813(2020)] applied the speaker's 11 unknowns theorem to obtain the following result.

Theorem. For the programming language SRL, there is no algorithm to determine for any SRL program P whether there is a tuple of inputs with length 12 which remains unaltered after the execution of the program P.

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

$$\begin{aligned} x < 0 &\iff x \neq 0 \wedge -x \geqslant 0 \\ &\iff \exists y_1(xy_1 = 1) \wedge \exists y_1 \exists y_3 \exists y_4 \exists y_5(-x = y_2^2 + y_3^2 + y_4^2 + y_5^2) \\ &\iff \exists y_1 \cdots \exists y_5[(x_9 y_1 - 1)^2 + (x_9 + y_2^2 + y_3^2 + y_4^2 + y_5^2)^2 = 0]. \end{aligned}$$

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`).

6. A. B. Matos, L. Paolini and L. Roversi, *The fixed point problem of a simple reversible language*, Theoret. Comput. Sci. **813** (2020), 143–154.

References (continued)

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

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

9. J. Richter-Gebert and U. Kortenkamp, *Complexity issues in dynamic geometry*, Foundations of Computational Mathematics, World Sci., 2002.

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

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

12. 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!