1. The Original Hilbert’s Tenth Problem

In 1900 D. Hilbert 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. At that time the exact meaning of algorithm was not known.

The theory of computability was born in the 1930’s. The problem whether \( n \) belongs to a given subset \( A \) of \( \mathbb{N} = \{0, 1, 2, \ldots\} \) is decidable, if and only if the characteristic function of \( A \) is Turing computable (or recursive). [In this case \( A \) is called a recursive set.] An r.e. (recursively enumerable) set is the empty-set \( \emptyset \) or the range of a recursive function, it is also the domain of a partial recursive function. It is well-known that there are nonrecursive r.e. sets. A relation \( R(a_1, \ldots, a_n) \) is said to be r.e. if the set

\[ \{ (a_1, \ldots, a_n) : R(a_1, \ldots, a_n) \text{ holds} \} \]

is r.e. A relation \( R(a_1, \ldots, a_m) \) is said to be Diophantine if there is a polynomial \( P(y_1, \ldots, y_m, x_1, \ldots, x_n) \) with integer coefficients such that

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

where variables range over \( \mathbb{N} \). A set \( A \subseteq \mathbb{N} \) is Diophantine if and only if the predicate \( a \in A \) is Diophantine. It is easy to show that a Diophantine set is an r.e. set.

In 1961 Davis, Putnam and J. Robinson [Ann. Math.] successfully showed that any r.e. set is exponential Diophantine, that is, any r.e. set \( W \) has the representation

\[ a \in W \iff \exists x_1, \ldots, x_n [P(a, x_1, \ldots, x_n, 2^{x_1}, \ldots, 2^{x_n}) = 0] \]
where $P$ is a polynomial with integer coefficients. Observe that the Fibonacci sequence \{F_n\} defined by

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

increases exponentially. In 1970 Matijasevič took the last step to show that the relation $y = F_{2x}$ is Diophantine. It follows that the exponential relation $a = b^c$ is Diophantine, i.e. there exists polynomial $P(a, b, c, x_1, \ldots, x_n)$ with integer coefficients such that

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

This surprising result together with the work of Davis, Putnam and Robinson leads to the following important result.

**Theorem 1.** Any r.e. set is Diophantine.

As some r.e. sets are not recursive, HTP over $\mathbb{N}$ is unsolvable, we also say that $\exists^n$ over $\mathbb{N}$ (with $n$ arbitrary) is undecidable. Lagrange’s theorem in number theory states that any $n \in \mathbb{N}$ can be written as the sum of four squares. Thus $P(x_1, \ldots, x_n) = 0$ has solutions over $\mathbb{N}$ if and only if

\[ P(u_1^2 + v_1^2 + y_1^2 + z_1^2, \ldots, u_n^2 + v_n^2 + y_n^2 + z_n^2) = 0 \]

has solutions over $\mathbb{Z}$. If $\exists^n$ over $\mathbb{Z}$ is decidable, then so is $\exists^n$ over $\mathbb{N}$. Now that $\exists^n$ over $\mathbb{N}$ is undecidable, so is $\exists^n$ over $\mathbb{Z}$, i.e. HTP is unsolvable!

It should be mentioned that a whole proof the unsolvability of HTP is very long and full of ingenious techniques. A modern proof given by J. P. Jones and Matijasevič [Amer. Math. Monthly, 1991] involves clever arithmetization of register machines.

Theorem 1 implies the following interesting result.

**Corollary 1.** Let $f$ be a recursive function of one variable. Then for some polynomial $Q(x, x_0, \ldots, x_n)$ with integer coefficients we have

\[ f(x) = y \iff \exists x_0, \ldots, x_n [Q(x, x_0, \ldots, x_n) = y]. \]

**Proof.** As the relation $f(x) = y$ is an r.e. relation, there exists a polynomial $P(x, y, x_1, \ldots, x_n)$ with integer coefficients such that

\[ f(x) = y \iff \exists x_1, \ldots, x_n [P(x, y, x_1, \ldots, x_n) = 0]. \]

Thus

\[ f(x) = y \iff \exists x_0, x_1, \ldots, x_n [1 - P^2(x, x_0, x_1, \ldots, x_n) > 0 \land x_0 = y] \]

\[ \iff \exists x_0, x_1, \ldots, x_n [(x_0 + 1)(1 - P^2(x, x_0, x_1, \ldots, x_n)) = y + 1] \]

\[ \iff \exists x_0, x_1, \ldots, x_n [Q(x, x_0, x_1, \ldots, x_n) = y] \]

where

\[ Q(x, x_0, x_1, \ldots, x_n) = (x_0 + 1)(1 - P^2(x, x_0, x_1, \ldots, x_n)) - 1. \]

It is well-known that a nonconstant polynomial $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ cannot always take prime values. However, we have the following surprising result.
Corollary 2. There exists a polynomial $Q(x_1, \cdots, x_n)$ with integer coefficients such that the positive integers in the range of $Q$ (variables run over $\mathbb{N}$) are just the primes.

Proof. Let $p_x$ denote the $x$th prime. Clearly the function $p_x$ is recursive. Applying Corollary 1 we then obtain the desired result.

2. Reduction of unknowns in Diophantine Representations

For a fixed nonrecursive set $W$, there exists a polynomial $P$ with integer coefficients such that

$$a \in W \iff \exists x_1, \cdots, x_\nu [P(a, x_1, \cdots, x_\nu) = 0].$$

Thus $\exists^\nu$ over $\mathbb{N}$ is undecidable. Note that here $\nu$ is a particular number (not an arbitrary number). To find the least $\nu$ with $\exists^\nu$ over $\mathbb{N}$ undecidable, is a very hard problem. In the summer of 1970 Matijasevič announced that $\nu < 200$, soon J. Robinson pointed out that $\nu \leq 35$. Then Matijasevič and Robinson cooperated in this direction, in 1973 they [Acta Arith. 1975] obtained that $\nu \leq 13$, actually they showed that any diophantine equation over $\mathbb{N}$ can be reduced to one in 13 unknowns. Among lots of techniques they used, here I mention the following one which can be used to reduce unknowns greatly.

Theorem 2 (Matijasevič-Robinson Relation-Combining Theorem). Let $k \in \mathbb{N}$. Then there exists a polynomial $M_k(x_1, \cdots, x_{k+4})$ with integer coefficients such that for any given integers $A_1, \cdots, A_k, B(\neq 0), C, D$ we have

$$A_1, \cdots, A_k \in \Box \text{ (the set of squares)}, \ B \mid C, \ D > 0$$

if and only if

$$M_k(A_1, \cdots, A_k, B, C, D, x) = 0 \text{ for some } x \in \mathbb{N}.$$

In 1975 Matijasevič announced further that $\exists^9$ over $\mathbb{N}$ is undecidable, a complete proof of this 9-unknowns theorem was given by Jones [J. Symbolic Logic, 1982].

As the original HTP is considered over $\mathbb{Z}$, what about the smallest $\mu$ such that $\exists^\mu$ over $\mathbb{Z}$ is undecidable? By Lagrange’s theorem, one natural variable can be expressed in terms of 4 integer variables. So, if $\exists^n$ over $\mathbb{N}$ ($n$ fixed) is undecidable, then so is $\exists^{4n}$ over $\mathbb{Z}$. This can be made better. Fermat called an integer in the form

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

a triangle number. He asserted that every natural number is the sum of three triangle numbers, i.e. we can write $n \in \mathbb{N}$ in the following form:

$$n = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2},$$
that is
\[ 8n + 3 = (2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2. \]

The Gauss-Legendre theorem states that \( n \in \mathbb{N} \) is the sum of three integer squares if and only if \( n \) is not of the form \( 4^a(8b + 7) \) where \( a, b \in \mathbb{N} \). It follows that for an integer \( n \) we have
\[ n \geq 0 \iff n = x^2 + y^2 + z^2 + z \text{ for some } x, y, z \in \mathbb{Z}. \]

[If \( 4n + 1 = a^2 + b^2 + c^2 \), then exactly one of \( a, b, c \) is odd, say \( 2 \nmid c \), thus \( a = 2x, b = 2y \) and \( c = 2z + 1 \) for some \( x, y, z \in \mathbb{Z} \).] Therefore the undecidability of \( \exists^n \) over \( \mathbb{N} \) implies the undecidability of \( \exists^{3n} \) over \( \mathbb{Z} \), thus S.P. Tung obtained the undecidability of \( \exists^{27} \) over \( \mathbb{Z} \) from the 9 unknowns theorem. In 1992 I improved this greatly

**Theorem 3** (Zhi-Wei Sun, 1992). (i) For any \( n \in \mathbb{N} \), if \( \exists^n \) over \( \mathbb{N} \) is undecidable, then so is \( \exists^{2n+2} \) over \( \mathbb{Z} \).

(ii) \( \exists^{11} \) over \( \mathbb{Z} \) is undecidable.

Part (i) was published in Z. Math. Logik Grundlag. Math. 38(1992). The result follows from my new relation-combining theorem for integers. Combining this with the 9 unknowns theorem we immediately get the undecidability of \( \exists^{20} \) over \( \mathbb{Z} \). The proof of part (ii) is very hard, though somewhat similar to the proof of the 9 unknowns theorem. To obtain a proof I use integer unknowns from the very beginning and study Lucas sequence
\[ u_0 = 0, \quad u_1 = 1, \quad u_{n+1} + u_{n-1} = Au_n \quad (n \in \mathbb{Z}) \]

with integer indices.

We remark that up to now no one can find \( P(x, y, z) \in \mathbb{Z}[x, y, z] \) such that
\[ x \geq 0 \iff \exists y \exists z[P(x, y, z) = 0]. \]

So, to replace a natural variable we need at least two more integer variables. In view of this, part (i) is interesting and part (ii) is difficult to be improved since \( 9 + 2 = 11 \). To express that \( x \) is nonzero we can use two integer unknowns only. S. P. Tung observed that
\[ x \neq 0 \iff \exists y \exists z[x = (2y + 1)(3z + 1)]. \]

3. **Classification of Quantifier Prefixes over Diophantine Equations**

We may also consider decidabilities of mixed HTP, that is, the quantifier prefixes over (polynomial) diophantine equation may contain universal quantifiers.

Let’s first consider the problem over \( \mathbb{N} \). It is easy to say that \( \exists \) is polynomial decidable. The decidability of \( \exists^2 \) is not known, though Baker found that a large
class of diophantine equations with two unknowns is decidable. In 1981 Jones proved that $\forall \exists$ is decidable, while the followings are undecidable:

$$\exists \forall \exists$$ (Matijasevič), $$\exists \forall \exists$$ (Matijasevič–Robinson), $$\exists \forall \exists, \forall \exists \exists \exists$$ (Jones).

The decidability of $\exists \forall \exists$ remains open. Recently, Dr. M. Rojas made progress in this direction. He showed that $\exists \forall \exists$ is *generically* decidable (co-NP), namely he gave a precise geometric classification of those $P \in \mathbb{Z}[x, y, z]$ for which the question

$$\exists x \forall y \exists z [P(x, y, z) = 0]$$

may be undecidable, and proved that this set of polynomials is quite small in a rigorous sense. He also showed that, if integral points on curves can be bounded effectively, then $\exists \forall \exists$ is generically decidable as well.

As for the problem over $\mathbb{Z}$, S.P. Tung [J. Algorithm, 1987] proved that $\forall^n \exists$ is co-NP-complete. I proved the undecidabilities of $\forall^{10} \exists$, $\exists^2 \forall \exists^3$, $\exists \forall \exists^4$ and so on.