Hilbert's Tenth Problem

– S. P. Suresh, CMI.
spsuresh@cmi.ac.in

Hilbert's Tenth Problem
– M Ram Murty
Brandon Fodden
AMS.

– Martin Davis (1973. AMM).

David Hilbert (1862–1943). 1900 – ICM.

23 problems.

Diophantus. (2nd Century CE).

$$6w + 2x^2 - y^3 = 0$$
$$5xy - z^2 + 6 = 0$$
$$w^2 - w + 2x - y + z - 4 = 0.$$

$w = 1, x = 1, y = 2, z = 4.$

$$6w + 2x^2 - y^3 = 0$$
$$5xy - z^2 + 6 = 0$$
$$w^2 - w + 2x - y + z - 3 = 0.$$

NO SOLUTION.

Spoiler: There is NO ALGORITHM to check whether a system of polynomial equations with integer coefficients has a solution in integers.

There is an algorithm to check for integer solutions

iff

there is an algorithm to check for non-negative integer solutions.

$P(x_1, \cdots, x_k) = 0$ has non-negative integer solutions

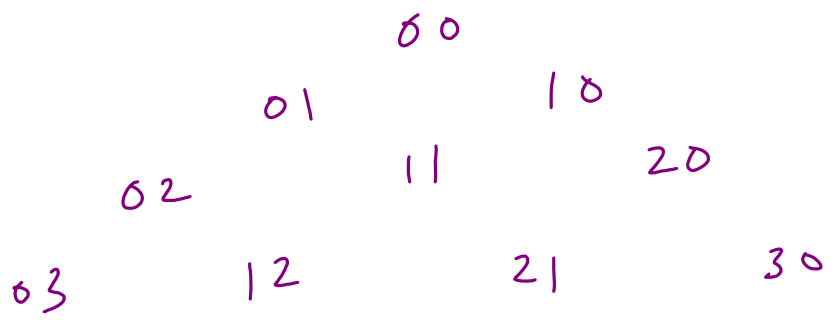
iff

$P(a_1^2+b_1^2+c_1^2+d_1^2, \cdots, a_k^2+b_k^2+c_k^2+d_k^2) = 0$ has integer solutions.

$P(x_1, \cdots, x_k) = 0$ has integer solutions

iff

$P(y_1 - z_1, \cdots, y_k - z_k) = 0$ has nonnegative integer solutions.



$$\boxed{x,y} \longrightarrow (1+2+\cdots+x+y)+x$$

$$= \frac{(x+y)(x+y+1)}{2} + x.$$

$P(x,y) \longrightarrow \underline{\underline{\langle x,y \rangle}}.$

$$\langle x,y,z \rangle = \langle x, \langle y,z \rangle \rangle.$$

$$\langle w,x,y,z \rangle = \langle w, \langle x,y,z \rangle \rangle.$$

$L(\omega)$, $R(\omega)$ —— the unique y s.t. $\exists x$ with $\langle x,y\rangle = \omega$.

$L(\omega)$: the unique x s.t. $\exists y$ with $\omega = \langle x,y\rangle$

Diophantine functions/sets/relations.

$S \subseteq \mathbb{N}$ is Diophantine if there is a $P(x,\vec{y})$ s.t.

$$S = \{x \in \mathbb{N} \mid \exists \vec{y}\ P(x,\vec{y}) = 0\}.$$

$R \subseteq \mathbb{N}^k$ is Diophantine if there is a polynomial $P(\vec{x},\vec{y})$ s.t.

$$R = \{\vec{x} \in \mathbb{N}^k \mid \exists \vec{y}\ P(\vec{x},\vec{y}) = 0\}.$$

$f: \mathbb{N}^k \to \mathbb{N}$ is Diophantine iff $\exists P$ s.t.

$f(\vec{x}) = y$ iff $\exists \vec{z}\,[P(\vec{x}, y, \vec{z}) = 0]$.

$\langle x, y \rangle = z$ iff $2z = (x+y)(x+y+1) + 2x$.

$x = L(z)$ iff $\exists y\,[2z = (x+y)(x+y+1) + 2x]$.

$y = R(z)$ iff $\exists x\,[$ " $]$.

Diophantine sets are closed under $\cap$ and $\cup$.

relations " $\wedge$ $\vee$.

$$\left[\exists \vec{y}\ P(\vec{x},\vec{y}) = 0 \ \wedge \ \exists \vec{z}\ Q(\vec{x},\vec{z}) = 0 \right]$$

iff

$$\left[\exists \vec{y},\vec{z}\ \left[P^2(\vec{x},\vec{y}) + Q^2(\vec{x},\vec{z}) = 0 \right] \right].$$

$$\exists \vec{y}\ P(\vec{x},\vec{y}) = 0 \ \vee \ \exists \vec{z}\ Q(\vec{x},\vec{z}) = 0$$

iff

$$\exists \vec{y},\vec{z}\ \left[P(\vec{x},\vec{y}) \cdot Q(\vec{x},\vec{z}) = 0 \right].$$

Example Diophantine sets / relations / fns.

- $x \mid y \iff \exists z\,[y = xz]$.
- $x \nmid y \iff \exists q r\,[y = xq + r \wedge 0 < r < x]$.
- $r < x \iff \exists z\,[x = r + z + 1]$.
- $r \leq x \iff \exists z\,[x = r + z]$.
- x is not a prime $\iff \exists y, z\,[(y+2)(z+2) = x]$.
- x is a prime $\iff \forall y < x\,[y = 1 \vee y \nmid x]$.

Gödel (1906–1978). There is a Diophantine function β s.t.

$\forall n \geq 0$ and all sequences $a_0, a_1, \ldots, a_{n-1}$, there is $u \in \mathbb{N}$ s.t.

$$\beta(u,i) = a_i \quad \forall i < n.$$

$$\beta(u,i) = rm\left(L(u),\ 1 + (1+i)\,R(i)\right).$$

$$rm(x,y) = r \iff \exists k\,[yk + r = x \wedge 0 \leq r < y].$$

$1, 1, 2.$

$\langle 1275, 6 \rangle.$

$$\begin{aligned} 1275 &\equiv 1 \mod 7 \\ &\equiv 1 \mod 13 \\ &\equiv 2 \mod 19. \end{aligned}$$

Strategy for the proof of unsolvability.

(1) Every computable function is Diophantine.

(2) Enumerate all Diophantine sets as $D_0, D_1, D_2, \ldots$

$$P_0 = 1.$$

$$P_{3i+1} = x_i$$

$$P_{3i+2} = P_{L(i)} + P_{R(i)}$$

$$P_{3i+3} = P_{L(i)} \cdot P_{R(i)}$$

$P(\vec{x}) = 0 \cdot \rightsquigarrow Q(\vec{x}) = R(\vec{x})$

positive coeff.

$\exists i, j$ s.t. $Q = P_i$, $R = P_j$.

$n = \langle i, j \rangle$.

$D_n = \{ x_0 \mid P_{L(n)}(x_0, x_1, \cdots, x_n) = P_{R(n)}(x_0, \cdots, x_n) \}$.

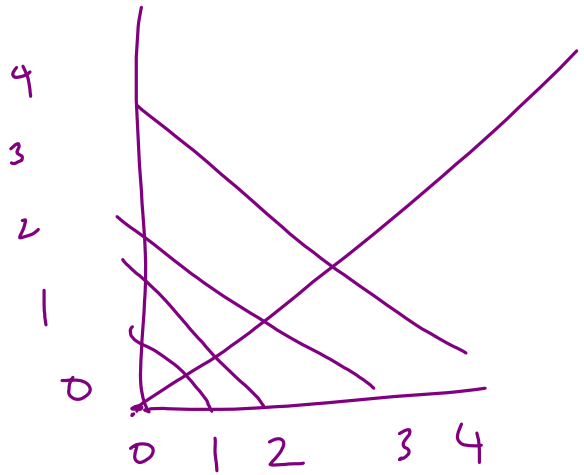
$U = \{(n, x) \mid x \in D_n\}$ is Diophantine.

$x \in D_n$ iff there is u s.t.

1. $\beta(u, 0) = 1$
2. $\beta(u, 1) = x$
3. $(\forall i \leq n)\left[\beta(u, 3i+2) = \beta(u, L(i)) + \beta(u, R(i))\right]$
4. $\forall i \leq n)\left[\beta(u, 3i+3) = \beta(u, L(i)) \cdot \beta(u, R(i))\right]$
5. $\beta(u, L(n)) = \beta(u, R(n))$.

$V = \{n \mid n \notin D_n\}$ is not Diophantine.

V is not computable



Suppose V is Diophantine.

Then $V = D_k$ for some k.

$k \in D_k \iff k \in V \iff k \notin D_k$. Contradiction!!

There is no algorithm to solve Diophantine equations.

If there is an algorithm, then we can "decide" V as follows.

apply the algorithm on $P_U(n, n, y_1, \dots, y_m)$. if the answer to this is "Yes" output "No".

if answer is "No", output "Yes".