Hilbert's 10^{th} Problem (H10):

Is there an algorithm with:

input: $f \in \mathbb{Z}[x_1, \ldots, x_n]$

output:

YES if $\exists \vec{a} \in \mathbb{Z}^n$ such that $f(\vec{a}) = 0$.

NO otherwise

Answer: NO

(Davis-Putnam-Robinson 1961, Matijasevič 1970)

(An algorithm is a) **Turing Machine** $\doteq$ a finite length computer program which accepts a non-negative integer input* and possibly prints characters to some output tape

$*$ or other kinds of inputs provided that an encoding is fixed.

Definition: $S \subseteq \mathbb{Z}$ is recursive $\iff \exists$ algorithm with:

input: $n \in \mathbb{Z}$

output:

YES if $n \in S$

NO if $n \notin S$

Example: $\{2, 3, 5, 7, \ldots\}$ is recursive.

Definition: $S \subseteq \mathbb{Z}$ is listable (recursively definable) $\Longleftrightarrow \exists$ Turing machine such that S is the set of integers it prints out when left running forever.

Proposition: Every recursive set $S \subseteq \mathbb{Z}$ is listable.

Proof: We're given an algorithm T to decide membership in S. Construct a Turing machine T' that applies T to

$$0, 1, -1, 2, -2, \ldots$$

in order, printing those that are in S.

Example: $S = \{a \in \mathbb{Z} \ : \ \exists x, y, z \text{ s.t. } x^3 + y^3 + z^3 = a\}$

Then S is listable:

```
for B = 1, 2, ...
    for x = -B to B
        for y = -B to B
            for z = -B to B
                print x^3 + y^3 + z^3
```

Is S recursive? Nobody knows.

Maybe

$$S = \{a \in \mathbb{Z} \quad : \quad a \not\equiv \pm 4 \pmod{9}\}?$$

If so, then S is recursive.

Halting Problem: Is there an algorithm with:

input: a computer program P and an integer x

output:

YES if program P when run on x eventually halts

NO otherwise

Answer: NO

Proof: Suppose there were an algorithm.

We could then write a new program H where H halts in input $x \iff$ program x does not halt on input x.

Taking $x = H$ gives a contradiction.

Corollary: $\exists$ listable set that is not recursive.

Proof: $S = \{x \;:\; \text{program } x \text{ halts on input } x\}$.

S is listable:

for $x = 1$ to N

simulate program x on input x for N steps

and print x if it halts (in N steps)

Is S recursive? NO.

If it were, we could repeat the construction of H in the proof of the Halting problem.

Diophantine Sets:

Definition $S \subseteq \mathbb{Z}^n$ is diophantine $\iff$

$\exists p(\vec{t}, \vec{x}) \in \mathbb{Z}[t_1, \ldots, t_n, x_1, \ldots, x_m]$ such that

$$S = \{\vec{a} \in \mathbb{Z}^n \quad : \quad \exists \vec{x} \in \mathbb{Z}^m \quad p(\vec{a}, \vec{x}) = 0\}$$

Examples:

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

   $\mathbb{N} = \{a \in \mathbb{Z} \;\; : \;\; \exists x_1, \ldots, x_4 \in \mathbb{Z} \quad a = x_1^2 + \cdots + x_4^2\}$

2. $\mathbb{Z} \setminus \{0\}$ is diophantine

   $a \neq 0 \iff \exists b, c \in \mathbb{Z}$ such that:

   $a = bc \qquad\qquad (b, 2) = 1 \qquad\qquad (c, 3) = 1$

$$\mathbb{Z} \setminus \{0\} = \left\{ \begin{array}{lll} a \in \mathbb{Z} & : & \exists b, c, p, q, r, s \text{ s.t.} \\ & & (a - bc)^2 + (bp + 2q - 1)^2 \\ & & +(cr + 3s - 1)^2 = 0 \end{array} \right\}$$

Proposition: Diophantine $\implies$ listable.

Theorem(DPRM): Diophantine $\iff$ listable.

Corollary: H10 has a negative answer.

Proof: Let $S \subseteq \mathbb{Z}$ be listable but not recursive.

$$\text{DPRM} \implies S \text{ is diophantine.}$$

$$\implies S = \{a \in \mathbb{Z} \ : \ \exists \vec{x} \ \ p(a, \vec{x}) = 0\}$$

If H10 had a positive answer, then we could decide membership in S.

But S is not recursive.

Corollary: $\exists\ F \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$\{F(\vec{a}) \quad : \quad \vec{a} \in \mathbb{Z}^n\} \bigcap \mathbb{Z}_{\geq 0} = \underbrace{\{2, 3, 5, 7, \ldots\}}_{\mathcal{P}}$$

Proof: $\mathcal{P}$ is listable $\implies$ (DPRM) $\mathcal{P}$ is diophantine.

$\mathcal{P} = \{a \in \mathbb{Z} \quad : \quad \exists \vec{x} \in \mathbb{Z}^n \quad p(a, \vec{x}) = 0\}$

Then $F(y_1, \ldots, y_4, x) := (1 - p(y_1^2 + \cdots + y_4^2, \vec{x})^2)(\underbrace{y_1^2 + \cdots + y_4^2}_{\geq 0})$

Outline of Proof of DPRM:

1. Prove that the 3-term relation

$$a = b^x \quad \text{on } \mathbb{Z}_{>0}$$

   is diophantine. (Uses Pell equation $x^2 - dy^2 = 1$)

2. $c = \binom{a}{b}$

   $\binom{a}{b} = \lfloor \frac{(x+1)^2}{x^b} \rfloor (\mathbf{mod}\ x) \quad \text{if } x > 2^a$

   $\{ \text{ bits of } a\} \subseteq \{ \text{ bits of } b\} \iff \binom{b}{a}$ is odd