Hilbert’s Problems

- In 1900 delivered address to International Congress of Mathematicians, identified 23 problems to (try to) solve in the next century.

- 10th problem:

  Devise an algorithm that tests whether a polynomial with integral coefficients has an integral root.

  \[ 6x^4 + 2^3 + 5x^5 + 4x^3 + x + 3 \]
Hilbert’s Problems

- In 1900 delivered address to International Congress of Mathematicians, identified 23 problems to (try to) solve in the next century.

- 10th problem:

  Devise an algorithm that tests whether a polynomial with integral coefficients has an integral root.

Today we know: no algorithm exists !!!
In 1936:
- Alonzo Church defines algorithms via $\lambda$-calculus
- Alan Turing defines algorithms via (decidable) TM's

**Church–Turing thesis:**

Intuitive notions of algorithms = TM algorithms

In 1970, Yuri Matijasevič (building on work of Martin Davis, Hilary Putnam, and Julia Robinson):

There is no algorithm for Hilbert's 10th problem.
Hilbert’s 10th problem in our terminology:

\[ D = \{ p \mid p \text{ is a polynomial with an integral root} \}, \]

where \( p \in \{0,1,...,9,x,+,-\}^* \).

Is it Turing-recognizable? \textbf{YES}

\[
\begin{array}{c c c}
6x^7 + 5x^3 + 3x^2z + \text{ } & \text{check if } p(x,z) = 0 \\
0 & 0 & 0 \\
0 & 1 & \leftarrow \text{just find a lexicographical order of the possible assignments and test them in this order} \\
1 & 0 & 0 \\
1 & 0 & 1 \\
-1 & 0 & \rightarrow \text{if one exists, the TM halts (accepts)} \\
-1 & 0 & \rightarrow \text{owl keeps going}
\end{array}
\]
A typical CS problem phrased in formal-languages way:

\[ A = \{ \langle G \rangle \mid G \text{ is a connected undirected graph} \}, \]

where \( \langle G \rangle \) is a string over \( \{0,1,|,(),\} \) describing a sequence of edges in the graph, e.g. \( \langle G \rangle = "(0|1)|(10|1)" \) denotes edges \((0,1)\) and \((10,1)\), vertices have identifiers from \( \{0,1\} \).

Is it Turing-recognizable / decidable? \( \text{both} \)

- do it just like in Java (e.g. BFS on the graph)
- but do it (painfully) on a TM
- (first check if \( \langle G \rangle \) encoded properly, otherwise reject)