Definition of Algorithm

• Algorithm: collection of simple instructions for carrying out some task (Sipser p 154)
• Hilbert: 23 mathematical problems for the new century (1900)
• 10th problem: devise algorithm that tests whether a polynomial has an integral root
  — no such algorithm exists
Algorithm

• Finding an algorithm: easy
• Proving no such algorithm exists: difficult
  – especially if you can't reason about/discuss an algorithm

• Different characterizations of algorithm:
  – Alonzo Church: algorithm as $\lambda$-calculus
  – Alan Turing: algorithm as machines
  – found to be equivalent

• Church-Turing Thesis
  – used to describe limits of computation
  – used on Hilbert's 10th problem

Hilbert's 10th Problem

• $D = \{ p \mid p$ is a polynomial with an integral root$\}$

• Hilbert: Is $D$ decidable?
  – No

• But it is Turing-recognizable
  – how could a TM recognize this language?
  – $6x^3y^2 - 2x - 3y - 1$
Terminology

• We care about algorithms, not TMs

• Descriptions
  – formal
  • full states and transitions
  – implementation
• English prose describes how the tape is used
  – high-level *

• English prose to describe an algorithm
• no implementation details

• Data : \( <G> \) an encoded piece of data, \( G \)
  – any data can be encoded as a string of 1s and 0s