“The conviction of the solvability of every mathematical problem is a powerful incentive to the worker. We hear within us the perpetual call: There is the problem. Seek its solution. You can find it by pure reason, for in mathematics there is no ignorabimus.”

David Hilbert, 1900

**Description**

We will exploit concepts and methods of computability theory and computational complexity theory to study several different problems of current research interest. Topics will include: Hilbert’s Tenth Problem, probabilistic algorithms, quantum computing, algorithmic learning theory. Other topics of particular interest to students in the class may be added, such as topics in Kolmogorov complexity, or in mathematical linguistics.

**Hilbert’s Tenth Problem:** “Is there an algorithm that determines whether any given Diophantine equation has a solution in integers?” was the only decision problem among twenty-three problems posed by David Hilbert at the Second International Congress of Mathematicians in 1900. This problem unifies, in a strikingly beautiful way, number theory and computability theory. It took seventy years to find its solution, and three-and-half decades to establish the mathematical theory of computability needed for the solution. Hilbert’s problem for equations in rational solutions still remains open.

**Quantum computing** is an emerging field. By exploiting quantum phenomena in physics that have no classical analogues, quantum computing is reinventing the foundations of computer science and information theory in a fascinating way. Unlike conventional computers, which work by manipulating bits that exist either in state 0 or 1, quantum computers encode information as qubits, which exist in a superposition of both states. Quantum algorithms
can be used to factor numbers fast—an extremely time-consuming problem when using a conventional computer. Like many quantum computer algorithms, Shor’s factoring algorithm is \textit{probabilistic}: it gives the correct answer with high probability, and the probability of failure can be decreased by repeating the algorithm.

\textit{Algorithmic learning theory}: We will adopt Gold-Putnam’s model of language acquisition known as identification in the limit. We will present explanatory learning (based on syntactic convergence) and behaviorally correct learning (based on semantic convergence), and will also study learning from all data (that is, learning from an informant), and learning from positive data only (that is, learning from text), as well as some intermediate concepts of learning.

\textbf{Required background}
Mathematical maturity and familiarity with the notion of an algorithm and basic logic and algebra. Math 272 can be taken for credit repeatedly. Advanced undergraduate students may also take this course for credit.

\textbf{Textbook}
Reading material will be provided in class.

\textbf{Grading}
Class participation, take-home assignments and their presentation.