Topics Covered: Sets, Functions, Number Theory, Formal Logic, Circuits, Counting, Probability, Graph Theory

Proofs: Proofs are the distilled goal of this course. Proofs are a convincing answer to the question “Why?”

Example: Are there infinitely many prime numbers?

1. Yes! ... but how do we know?

2. We can have different levels of answering this question:
   (a) Yes, because I believe it.
   (b) Yes, because my teacher told me.
   (c) Yes, because I can prove it by contradiction!

Proof techniques we will look at:

1. Direct proofs
2. Proofs by contradiction
3. Induction
4. Probabilistic proofs:
   (a) You are trying to show a computer program does what you say it does. How many times do you have to run it and show it works before you are convinced?
   (b) Colorblind proof: How many times would you have to distinguish between two differently colored marbles to convince someone who is colorblind that you can distinguish between these two marbles?
   (c) Proving that cards have been shuffled well – you should not be able to tell where the cards are. How do you convince someone that cards have not been well shuffled? Can show it mathematically. Or show someone that you can predict the cards in a deck!

5. Zero Knowledge Proof – Suppose you want to convince someone of something without giving them any knowledge.
(a) Applications in cryptography – Can you convince someone you have a certain password without giving it to them?

(b) Where’s Waldo example – Can you convince someone that you know where waldo is without telling them?

Why do we know things?

Many people know powers of two, not many people know powers of three. Why?

Powers of two count familiar things! For example, $2^n$ counts the number of binary strings of length $n$.

Check:
$2^1 = 2$ and number of strings of length 1 is 2: 1, 0.
$2^2 = 4$ and number of strings of length 2 is 4: 10, 00, 01, 11.