Class Notes: 1/23

Class Intro

Lots of topics:

- Preliminaries, Sets, Relations
- Number Theory
- Logic
- Counting and Probability
- Graph Theory

The actual point is to develop mathematical maturity.

Powers of 2

Computer scientists know many powers of 2, but they don’t know powers of 3.
We know this because our computers work with binary. Audience is important!

Infinite Primes

Break numbers into smaller parts (they are products of these parts). Looking at building blocks for addition, we have everything as a sum of ‘1’s.

For multiplication, we’re claiming there are an infinite number of building blocks for multiplication.

If we said there were a finite number of them, then we claim that every number can be expressed as products of those.

Being Convincing

This leads to us talking about how we can convince people of things, a very important skill no matter what you do.

There are many kinds of proofs!
In some contexts we need to prove things “beyond a reasonable doubt”. This isn’t always used in math, but for mathematical claims we do this too!

Now, there is a style of proof called a probabilistic proof in modern day computer science. Here, we prove things are true with “strong” confidence. This entails constructing experiments that help convince people using probability and likelihood.

- Coin flipping example with bias
- Card shuffling machine at a casino

**Zero-knowledge Proof**

Convincing someone you know information without having to share the information. Example: I want to convince you that I know your password without actually giving it to you.

Uses number theory and logic (topics we will cover).

Where’s Waldo example. I want to convince you that I know where Waldo is without pointing at him. I can do this by first getting a big poster board. I cut out an outline of Waldo and put the board down so that you can see Waldo without knowing where Waldo is compared to the rest of the paper.