# Recitation Notes

H241: Discrete Structures

*Spring Term 2025*

## 1/17/2025

Recitation held over Zoom with Prof. Leivant (I was out of town). Notes are available on the Course Material page.

## 1/24/2025

The plan for today:

- Check in, how are you all doing?
- Homework questions
- Talk about different proof strategies

Let's take a pause from sets and relations for a moment. For most of you, this is probably the first maths class where you've been expected to prove claims from scratch. We expect your proofs to look pretty much like what you've seen in class and on the solved homework examples. Any logically sound argument from premise to goal counts as a proof. It's good to write in a conversational tone, but at least in the beginning it's important to show every step, and make sure each sentence logically follows the previous one.

We will take a moment now to review the different types of proofs we've seen:

**Proof by Construction / Example.** If you are asked to show "there exists some X with property P(X)" (or "there is", or "define"), then all you need to do is *give a construction / give an example*! It's important to make sure to check that P(X) is actually true.

- **Example:** Show that there are primes $p, q$ that are twin primes, i.e. $|p - q| = 2$.
  **Proof:** 3 and 5 are twin primes. We can check: $|3 - 5| = 2$ ✔

Similarly, if you're asked to show "not every X has property P(X)", all you need to do is *give a counterexample*, and check that P(X) holds for that counterexample.

**Direct Proof.** If you're asked to show "every X has property P(X)", then pick an arbitrary X (all you can assume about it is given by its definition), then show that P(X) holds. The same principle applies when proving implications "if X then Y"—suppose X, then prove Y.

- **Example:** Show that all primes $p > 2$ are odd.
  **Proof:** Let $p > 2$ be prime. By definition of prime, $p$'s only divisors are $p$ and 1. In particular, none of its divisors are 2. So $p$ must be odd.

**Proof by Contradiction.**

- **Example:** Show that all primes $p > 2$ are odd.
  **Proof:** Let $p \geq 2$ be prime, and suppose for contradiction that it's even. That is, $p = 2m$ for some integer $m > 0$. We have two cases:

***m* = 1.** So $p = 2$. But $p > 2$ (a contradiction!)

***m* > 1.** So $p$ is divisible by 2 and some $m > 1$. But this contradicts the fact that $p$ is prime.

Prof. Leivant (and many computer scientists) prefer to avoid proofs by contradiction because they aren't *constructive*, i.e. they don't show you how to actually get to the conclusion from the premise.

**Proof by Cases.** The above proof also demonstrates a "proof by cases". If our goal is to prove X, we can choose to split into cases. So long as we cover all possible cases (e.g. we consider both P and not-P, or we consider $m = 1, m < 1, m > 1$, etc.), and prove X in each case, we have proven X in general. In general, this proof technique is also not constructive.

**Proof by Contraposition.** Here's a general logical principle which we take as sound: X implies Y iff *not*-Y implies *not*-X. Sometimes it's easier to prove that not-Y implies not-X! (Note that in general, this proof technique is also not constructive.)

- **Example:** If $r$ is irrational, then $r^{\frac{1}{5}}$ is irrational.

  **Proof:** Let's prove the contrapositive: If $r^{\frac{1}{5}}$ is rational, then $r$ is rational. Suppose $r^{\frac{1}{5}}$ is rational, i.e. $r^{\frac{1}{5}} = \frac{a}{b}$ where $a, b$ are integers and $b \neq 0$. So

  $$r = \left(r^{\frac{1}{5}}\right)^5 = \left(\frac{a}{b}\right)^5 = \frac{a^5}{b^5}$$

  Since $a$ is an integer, so is $a^5$, and similarly for $b$. So $r$ is rational.

In class we showed that $\sqrt{2}$ is irrational. Let's put all these techniques together to show:

**Proposition.** There exist irrational numbers $a, b$ such that $a^b$ is rational.

**Proof.** Instead of actually giving $a$ and $b$, we can (nonconstructively) split into two cases, and in each case find a different $a^b$. (This proof is cute, but unsatisfying in the sense that we never really say which world we're actually in. This is one reason why many computer scientists prefer constructive/direct proofs).

**Case 1.** $\sqrt{2}^{\sqrt{2}}$ is rational. In this case, let $a = \sqrt{2}, b = \sqrt{2}$. We have $a^b = \sqrt{2}^{\sqrt{2}}$, which is rational.

**Case 2.** $\sqrt{2}^{\sqrt{2}}$ is irrational. In this case, let $a = \sqrt{2}^{\sqrt{2}}$, and let $b = \sqrt{2}$. We have

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$$

which is rational.

□