Math 95: Transition to Upper Division Mathematics, Part I

Michael Andrews
UCLA Mathematics Department

September 13, 2018

Contents

1 Introduction

1.1 My goal for this class

What do I like least in a (math) classroom? When my students don't talk!

When my students don't talk to me, I don't know whether they are confused or bored. If I can tell that they are confused, I still don't know *when* they became confused or *what* confused them. Was the previous two weeks worth of material overwhelming, or was it the last five minutes? Have I made a mistake on the board? Is it that which is causing confusion? Oh wait, finally someone pointed it out - silly old me! (I officially become old this birthday.) I wish someone had spoken up 20 minutes ago when they were first confused!

There are many reasons that I can think of for students to be hesitant to speak out. In class, I'll make a note of the reasons that *you* think of. Here are **your reasons for not speaking up in *previous* classes**:

1. Apppearing "stupid."

   - Isn't this part of learning? We're human. We make mistakes and say silly things sometimes. Perfection is an unrealistic goal in every day life.

2. The class is hard.

   - I saw this as a great reason for talking. It suggests that "stupid" might be the default since everyone is a little confused. You'll have to work harder to do well in such a class. And talking is part of working.

3. Mean professor.

   - Hopefully I'm not. But I will have to say when your ideas or proofs are incorrect. So will your fellow students. The fact that things in math are correct or incorrect is actually kind of comforting. It is far easier to move on from being wrong in math, than it is when you upset a friend for behaving in some way that you feel bad about.

4. Bad teacher.

   - We'll see.

5. Am I annoying others with my questions?

   - Who is paying for *your* education? You or them? You are entitled to ask questions if you wish. The lecturer will make sure your questions are not disruptive. You are simply trying to maximize your learning.

6. Laziness.

   - Class is so much less of a chore if you're engaged. Also, remember who's paying. I often use this to motivate myself to go boxing when I don't feel like it.

7. If the teacher asks something and I don't know the answer.

   - Do you fully understand the question though? If not, it could be good to clarify, particularly if someone is about to answer it. You are not going to get very much from their answer if you don't understand the question. If you do understand the question, then it might be a good moment to be quiet. Or maybe ask for a hint? The lecturer could just be trying to assess the general understanding of the room.

8. What I wanted to say has already been said.

   - That seems like a good reason, and a good point at which to move on.

Hopefully, I'll be able to convince you that although you're certainly not wrong for feeling your feelings, there is a better way, and that is to talk lots. In fact, while I hope you come out of this class having learned some proof-writing and some interesting mathematics, my biggest goal is to create an environment where you feel comfortable speaking out in class, office hours, and that, by the end, you feel like you learned how to optimize your learning in a math class. I hope that this list of *the most important things that I learned in grad school* might start helping you to be less quiet.

- I am in control of my learning. How much I participate usually corresponds with how much I enjoy a class and how much I learn in the class.
- Asking a question earlier rather than later usually results in less confusion on my part.
- If I am confused, it is likely that half the room is confused too, and my question will probably help others. It can help in two ways.
  - Directly, by clearing up a mistake or something that the lecturer said unclearly.
  - Indirectly, by calling the lecturer's attention to the fact that people are confused, forcing a flexible lecturer to try to change something.
- My "stupid" questions are usually my most important questions and it makes me feel better if I do not think of them as "stupid."
- Math is really difficult, and on some days it feels worse than others. It's better to be kind to myself on such days, and to ask the people who are explaining ideas to me to slow down or explain things more thoroughly if necessary.
- The lecturer probably likes questions.

1.2 Flipped classroom

This course will make use of a *flipped classroom.* In short, this means that you are going to be talking a lot. Well, at least I hope that you will. Please. Please talk. Please. One more... Please!!

Our class time is 9:00-10:50am. From 10:00-10:50am, I will introduce new concepts, and state theorems. Sometimes I will also prove things, so that you can see how I do it.

The start of class, 9:00-9:50am is for you to present proofs of theorems that I have stated the lecture before. It is not completely set in stone how this will work. We might try a few things to see what works best.

One idea I have is for 3 of you to come up at a time and write your proofs of the same theorem. By taking the best parts of each proof, we can construct the best proof possible. By seeing the parts of proof-writing that others do well, and that others do less well, you will become more self-aware with regard to how your own proofs might be interpretted by others.

1.3 Participation

The success of the flipped classroom is strongly dependent on your willingness to participate. You will be graded on your participation, and so your success in the class is also dependent on such a willingness.

How will I assign a score for your participation? Read ahead.

1.3.1 Your participation score

Various things that you do in the class will give you points. Most important will be the points that you receive for presenting in class, and asking questions in class.

I'll use these points to rank you.

Then I'll use some increasing function from class rank to $\{0, 1, 2, \ldots, 19, 20\}$.

Since I have never done this before, I cannot say precisely what this function will be. But I would hope for at least half the class to receive scores in $\{16, 17, 18\}$, and a few in $\{19, 20\}$. A dream class would have no-one scoring below 14, but it is summer, and I'd be very pleasantly surprised if no-one spent the quarter slacking off!

1.3.2 Presenting in class

We have 17 scheduled classes. You will not present the first day, the day of the midterm, or on the last day of class. So there are 14 classes in which you, as a class, will present. If we aim for at least 6 people presenting each class. That works out as each person presenting 3 or 4 times.

Each time you present, you will receive a score out of 4.

1. 1 point is for presenting.

2. 2 points indicates that a significant step was made towards proving the result.

3. 3 points indicates that all the ideas of your proof were correct, and that the class and I were convinced of your proof.

4. 4 points will be awarded if your proof is correct, clearly written, and the only ways that I can see to improve upon it are subjective, and completely a matter of my personal taste. I'll have Kevin look too.

Some of the things that I ask you to prove in the class will be quite difficult. Since class time is for learning, I don't expect your proofs to be perfect. If everyone is receiving 4's every time, then there's no need for the class! I expect the most common score I will give will be a 2. So please don't feel disappointed with a 2. 3 is an excellent score. I expect to give out very few 4's. They are an indication of an A+ worthy effort. To be honest, most proofs I write (at this level of mathematics) would probably result in a 3. There's almost always a way in which I could improve a proof.

If you receive 1 point, there is some work to do, but this will not necessarily result in a poor participation score at the end. If you put in the work to understand why your proof did not make a significant step towards proving the result, I will make a note of this. Also, you can always speak to me about presenting again in the near future, or presenting to me another time. Bear in mind, however, that class time and my time is not infinite!

A priori, I would be willing to give a score of 15/20 to someone with scores of 1,2,2,3, 18/20 to someone with scores of 2,2,3,3, and 20/20 for someone with scores of 2,3,3,3. But it does depend on the standard of the class, and in my ability to give you reasonably accessible yet challenging and useful theorems to prove.

1.3.3 Asking questions in class and tickets

I will have a roll of raffle tickets. Each class, you have the opportunity to receive two raffle tickets: one in the first part of the class when students are presenting, one in the second part of class when I am lecturing. At the end of the quarter, the person with the most raffle tickets will receive my guitar. jk. My guitar is going nowhere.

You will receive a raffle ticket for almost any math question which is related to the current or previous material we have covered. You can staple your raffle tickets to the homework you turn in so that Kevin can record how many tickets you received each week. These will contribute to your participation score.

1.3.4 Question box in class

In the break between students presenting, and me lecturing, I will pass around a box. In that box please post either

- a blank bit of paper,
- an anonymous bit of paper with a question on it, or
- a question with your name on it.

I'll look at these before we resume.

The reason for the blank bit of paper, is so that everyone looks like they are doing the same thing. The reason for the anonymous bit of paper is to allow you to ask a question if you're worried about me judging you (I'll only judge your music taste). The reason for a bit of paper with your name on it is so that I can give you participation credit for your question. I won't reveal who asked the question to the rest of the class, in case you're embarassed by the question.

1.3.5 Presenting in office hours

I'd like to give people the opportunity to present in office hours too. However, this depends on it seeming like an appropriate use of time. If there are people there confused by concepts I've covered in class, it would seem best to focus on clearing up that confusion. If what I said in lecture is well understood, but proof-writing needs attention, someone wants to present, and others are happy to comment, then we can do this. In this case, I am happy to award points for presenting, and raffle tickets for the question-asking that happens.

Notice that sitting in office hours but saying nothing does not receive any participation points. If you're shy, send me or Kevin an email. I hope that after talking with us solo for a bit, you'll feel more comfortable talking in front of the other students.

1.4 Discussion

I have let Kevin run his discussions however he sees fit. He might try an online group chat which runs during class. It is likely that he will experiment with group work. Although I didn't mention group work above, I might also play with this in class, especially if Kevin finds it productive. I'll leave it to Kevin to explain himself when he meets you.

You should ask Kevin if he's going to grade your last homework.

1.5 Homework

There will be five homeworks. They are **due on Mondays at the start of class** starting in week 2. The *lowest* homework score will be dropped.

1.6 Midterm

There will be one midterm on **Monday 27th August**.
It will take place in the first 60 minutes of class.

1.7 Final

The final exam will take place on **Thursday 13th September**.
The exam will be 2 hours long and will take place in discussion.

1.8 Grading

From your participation, homework, quizzes, and final, two scores will be calculated for you using the following schemes:

	Scheme 1	Scheme 2
Participation	20%	25%
Homework	20%	20%
Midterm	25%	15%
Final	35%	40%

Your final score will be the *higher* of those two scores.
You will be assigned a letter grade using your class rank.

Any issues about grading must be addressed within *two weeks*. After that time no score changes will be allowed. Scores will be available online through `my.ucla.edu`.

1.9 Office hours

Office hours are posted on the website: `math.ucla.edu/~mjandr/Math95`.

2 Lecture on August 6th: Cantor and sets

2.1 Cantor

This class is called "Transition to Upper Division Mathematics." There is no better place to begin than when humans made the transition to "upper division" mathematics. They did not find this an easy transition...

`http://en.wikipedia.org/wiki/Georg_Cantor`

The objections to Georg Cantor's work were occasionally fierce: Henri Poincaré referred to his ideas as a "grave disease" infecting the discipline of mathematics, and Leopold Kronecker's public opposition and personal attacks included describing Cantor as a "scientific charlata," a "renegade" and a "corrupter of youth." Cantor's recurring bouts of depression from 1884 to the end of his life have been blamed on the hostile attitude of many of his contemporaries.

The harsh criticism has been matched by later accolades. In 1904, the Royal Society awarded Cantor its Sylvester Medal, the highest honor it can confer for work in mathematics.

What did Cantor give to mathematics that caused such controversy?

When we are young, the first piece of mathematics we learn is counting:

$$1, 2, 3, \ldots$$

We quickly find out in the playground that it is always possible to win the game of choosing the biggest number *as long as we go second.* We can always add 1 to the other player's number. The natural numbers go on forever. There are infinitely many of them.

Until Cantor's work it was thought that sets either had "size" equal to 0, a natural number, or that they were infinite, and that the story ends there. That's not very good is it? A story about infinity, and it ends very quickly with us declaring that everything is either finite or infinite.

Cantor showed that there are an inifinity of infinities and he developed the language to talk about this precisely! Talking about "size" precisely is actually necessary for this result to be interesting, since otherwise it just sounds like the words of some stoner who discovered the complete works of Johann Sebastian Bach (there are over 1000 known compositions by Bach).

If you are going to show that there are infinitely many of something, then you better be able to show that there are two of that something. So can we even specify two sets whose "size" is infinite, but where their sizes are not equal? Yes-ish! We already have one infinite set: the *natural numbers*

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Another infinite set is the set $\mathbb{R}$ containing the *real numbers.* Amazingly, the infinity of the size of the real numbers is strictly bigger than the infinity of the size of the natural numbers. But wait. Maybe you do not think that is amazing? Isn't it obvious because every natural number is a real number? Well, is the size of the set of *integers*

$$\mathbb{Z} = \{0, -1, 1, -2, 2, \ldots\}$$

bigger than the size of $\mathbb{N}$? Maybe you think it is weird that the answer to this is "no." They have the same size because we can pair up their elements.

$$\begin{tikzcd}
\mathbb{N} \arrow[d, leftrightarrow] & 1 \arrow[d, leftrightarrow] & 2 \arrow[d, leftrightarrow] & 3 \arrow[d, leftrightarrow] & 4 \arrow[d, leftrightarrow] & 5 \arrow[d, leftrightarrow] & 6 \arrow[d, leftrightarrow] & 7 \arrow[d, leftrightarrow] & \ldots \\
\mathbb{Z} & 0 & -1 & 1 & -2 & 2 & -3 & 3 & \ldots
\end{tikzcd}$$

You can *not* pair up the elements of $\mathbb{N}$ and $\mathbb{R}$. Cantor drops the mic.

In class, we spoke about this for longer, and our discussion emphasized that not having precisely defined concepts makes talking about such things quite confusing. This is good motivation for where we are heading.

2.2 Sets

Definition 2.2.1. A *set* is a collection of mathematical things. The members of a set are called its *elements*. We write $x \in X$ to mean that "x is an element of a set X."

Definition 2.2.2. We often use curly brackets (braces) for sets whose elements can be written down easily. For example, the set whose elements are $a_1, a_2, a_3, \ldots, a_n$ is written as $\{a_1, a_2, a_3, \ldots, a_n\}$, and the set whose elements are those of an infinite sequence $a_1, a_2, a_3, \ldots$ is written as $\{a_1, a_2, a_3, \ldots\}$.

Remark 2.2.3. Some infinite sets can not be written out in an infinite sequence. This is one of Cantor's results. This means that not all sets can be described using the notation just defined. An example is the set of real numbers. Eventually, you'll prove this to me!

Definition 2.2.4. We often describe a set as "elements with some property." For example, the set of elements with a property P is written as $\{x : x \text{ has property } P\}$, and the elements of a previously defined set X with a property P is written as $\{x \in X : x \text{ has property } P\}$.

Remark 2.2.5.

- In the previous definition the colons should be read as "such that."
- The second way of describing a set $\{x \in X : \ x \text{ has property } P\}$ is much better than the first because the first allows for Russell's paradox: the "set" $\{A : \ A \text{ is a set and } A \notin A\}$ makes no sense! `http://en.wikipedia.org/wiki/Barber_paradox#Paradox`

Notation 2.2.6. Here is some notation for familiar sets. ":=" means "is defined to be equal to."

1. the *empty set* $\emptyset := \{\ \}$ is the set with no elements,
2. the *natural numbers* $\mathbb{N} := \{1, 2, 3, \ldots\}$,
3. the *integers* $\mathbb{Z} := \{0, -1, 1, -2, 2, -3, 3, \ldots\}$,
4. the *rationals* $\mathbb{Q} := \{\frac{m}{n} : \ m \in \mathbb{Z}, \ n \in \mathbb{N}\}$,
5. the *reals* $\mathbb{R}$,
6. the *complex numbers* $\mathbb{C} := \{x + iy : \ x, y \in \mathbb{R}\}$.

Definition 2.2.7. Suppose X and Y are sets. We say that X is a *subset* of Y **iff** whenever $z \in X$, we have $z \in Y$. We write $X \subseteq Y$ to mean "X is a subset of Y."

Remark 2.2.8. In this definition "iff" stands for "if and only if." This means that saying "X is a subset of Y" is exactly the same as saying "whenever $z \in X$, we have $z \in Y$."

Often, in definitions, mathematicians say "if" even though the meaning is "iff." I normally do this, and I feel a little silly for writing "iff," but I decided that it's the least confusing thing I can do. To make this "**iff**" feel different from a non-definitional "iff" I have used bold.

Definition 2.2.9. Suppose X and Y are sets. We say that X is *equal to* Y **iff** X is a subset of Y and Y is a subset of X. We write $X = Y$ to mean "X is equal Y."

Example 2.2.10.

1. $\{0, 1\} = \{0, 0, 0, 1, 1\} = \{1, 0\}$.
2. Suppose X is any set. Then $\emptyset \subseteq X$.
3. $\emptyset \neq \{\emptyset\}$. This is because $\emptyset \notin \emptyset$ and so $\{\emptyset\} \nsubseteq \emptyset$.
4. $\{n \in \mathbb{N} : n \text{ divides } 12\} = \{1, 2, 3, 4, 6, 12\}$.

3 Student proofs on August 7th

Theorem 3.1. *Let $n \in \mathbb{N}$. There are ??? different subsets of* $\{1, 2, \ldots, n\}$.

Fill in the ??? correctly and prove your result. Remember that $\emptyset \subseteq \{1, 2, \ldots, n\}$.

I purposefully haven't told you what a proof "should" look like. I can think of a few different proofs with varying levels of detail. Funnily enough, more details don't always make a better proof. My favorite proof of this result is basically a short and clear explanation of why the result is true. I am interested to see the different proofs that students come up with.

If you are struggling, don't look up a proof. First, count the number of subsets of $\{1, 2, \ldots, n\}$ for a few different values of n. Then see if you can spot a pattern. Then see if you can explain the pattern that you spotted.

Theorem. *Let $n \in \mathbb{N}$. There are 2^n different subsets of* $\{1, 2, \ldots, n\}$.

Andrew's proof. For $\{1\}$ the subsets are $\{1\}$ and $\emptyset$. 2.

For $\{1, 2\}$ the subsets are $\{1, 2\}$, $\{1\}$, $\{2\}$ and $\emptyset$. $4 = 2^2$.

For $\{1, 2, 3\}$ the subsets are $\{1, 2, 3\}$, $\{1, 2\}$, $\{2, 3\}$, $\{1, 3\}$, $\{3\}$, $\{2\}$, $\{1\}$, $\emptyset$. $8 = 2^3$.

It looks as though for $\{1, 2, 3, \ldots, n\}$ the number of subsets are 2^n.

We must demonstrate that 2^n holds for $(n + 1)$ case using induction.

Assume base case: 2^n is the number of subsets for $\{1, 2, \ldots, n\}$.

Let $X := \{1, 2, \ldots, n\}$ and $P = \{1, 2, 3, \ldots, n + 1\}$. Then $P = X \cup \{n + 1\}$ where $n + 1 \notin X$.

There are 2^n subsets $S \subseteq X$ and by definition of $\cup$, each subset S creates two subsets of P, $S \cup \{n + 1\}$ and S itself.

Therefore the number of subsets of P is $2 \cdot 2^n = 2^{n+1}$.

The number of different subsets of $\{1, 2, 3, \ldots, n\}$ is 2^n since it holds for $\{1, 2, 3, \ldots, n + 1\}$ case. □

Remark 3.2. I think this proof is a very good attempt at an inductive proof, and I could definitely understand the idea and see that it works correctly. Two criticisms are:

1. Andrew did not introduce the result he was proving explicitly.

2. The induction was not written up completely correctly. We will certainly cover induction at some point this quarter, so I don't want to get hung up on this now. It is okay if you have not seen induction before.

Below I edit Andrew's proof to be entirely correct. In class, I explained (particularly for those of you who have not seen induction) the idea in Andrew's "inductive step" in a specific case of n. I have incorporated this into his proof as well.

Michael's edit of Andrew's proof. For $n \in \mathbb{N}$, we wish to show there are 2^n subsets of $\{1, 2, \ldots, n\}$.

First, we make some observations which might help the reader to understand our proof.

There are two subsets of $\{1\}$: $\emptyset$ and $\{1\}$.

Both of these sets are also subsets of $\{1, 2\}$. By adding the element 2 to each of the two sets, respectively, we obtain two other subsets of $\{1, 2\}$: $\{2\}$ and $\{1, 2\}$. In total there are four subsets of $\{1, 2\}$: $\emptyset$, $\{1\}$, $\{2\}$, and $\{1, 2\}$.

Each of these four subsets is also a subset of $\{1,2,3\}$. By adding the element 3 to each of the four sets, respectively, we obtain four other subsets of $\{1,2,3\}$: $\{3\}$, $\{1,3\}$, $\{2,3\}$, and $\{1,2,3\}$. In total there are eight subsets of $\{1,2,3\}$: $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1,2\}$, $\{2,3\}$, $\{1,3\}$, $\{1,2,3\}$.

By using the idea that we employed twice above, we can write an inductive proof that there are 2^n subsets of $\{1,2,\ldots,n\}$.

The base case is when $n=1$, that there are two subsets of $\{1\}$. This is true because there is $\emptyset$ and $\{1\}$ (as we already remarked above).

For the inductive step, assume that $n \in \mathbb{N}$, and that it is true that there are 2^n subsets of $\{1,2,\ldots,n\}$. We wish to prove, under this this assumption, that there are 2^{n+1} subsets of

$$\{1,2,\ldots,n,n+1\}.$$

The key observation is that subsets of $\{1,2,\ldots,n,n+1\}$ either contain $n+1$ or they do not. If a subset does not contain $n+1$, then it is one of the 2^n subsets of $\{1,2,\ldots,n\}$. If it does contain $n+1$, then then it is one of the 2^n subsets of $\{1,2,\ldots,n\}$ with $n+1$ added. For this reason, we have $2 \cdot 2^n = 2^{n+1}$ subsets of $\{1,2,\ldots,n,n+1\}$ in total. This completes the proof of the inductive step.

We have now completed the inductive proof of the theorem. □

Alvin's proof. Let H be a set with n elements.

Let B be a subset of H with p amount of elements.

So $0 \le p \le n$ where p and n are whole numbers.

Since B is a subset of H all its numbers must come from H.

Counting the amount of subsets for a given p,

$$\underbrace{n \cdot (n-1) \cdot (n-2) \cdots}_{p}$$

is the total amount of combinations with n elements but only choosing p amount $\longrightarrow \frac{n!}{(n-p)!}$.

But this includes something like $\{a,b,c\}$ and $\{b,c,a\}$, but $\{a,b,c\} = \{b,c,a\}$, so it's counted multiple times. To remedy this divide by $p!$.

So now we have the correct amount of subsets with p elements $\frac{n!}{(n-p)!p!} = \binom{n}{p}$.

We need to add the amount of subsets from 0 to p, so $\sum_{p=0}^{n} \binom{n}{p}$. □

Remark 3.3. I think this is a very good attempt at a combinatorial proof, and I could definitely understand the idea and see that it works correctly. Some criticisms are:

1. Alvin did not introduce the result he was proving explicitly.

2. Proving a slightly more general result (one about an arbitrary n element set H instead of the set $\{1,2\ldots,n\}$) could confuse some readers. There could be a comment about this.

3. The "counting" formula that Alvin uses almost explains itself, but it is possible to make the explanation a little more explicit. Maybe the $p=0$ should be done separately.

4. Generally, a little more care could be taken with language, but I was very happy with the use of words rather than unexplained formulae.

Below I edit Alvin's proof to account for these comments.

Remark 3.4. Because of the binomial theorem $2^n = (1+1)^n = \sum_{p=0}^{n} \binom{n}{p}$.

So Alvin's answer agrees with Andrew's answer. I think we would all agree Andrew's answer is more concise. But sometimes when conjecturing and proving a result, you might not come up with the optimal theorem first time. This is fine. Lots of the math you will learn in undergraduate took many years to be refined into the form in which it is now taught and learned.

Michael's edit of Alvin's proof. Let $n \in \mathbb{N}$ and suppose that H is a set with n elements. We will prove that H has $\sum_{p=0}^{n} \binom{n}{p}$ elements, where

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}.$$

This is slightly more general than the statement of the theorem which concerns the set $\{1, 2, \dots, n\}$.

The number of elements in a subset of H is an integer between 0 and n. So let $p \in \{0, 1, \dots, n\}$. First, we will count the number of subsets B with size p and show it to be $\binom{n}{p}$.

When $p = 0$, there is only one subset of size p (the empty set). Morever, $1 = \binom{n}{0}$.

Suppose $p > 0$. Let's think about picking p distinct elements from H. There are n choices for the first element, leaving $n-1$ choices for the second element, leaving $n-2$ choices for the third element, and so on. That gives us

$$n(n-1)(n-2)\cdots(n-p+1) = \frac{n!}{(n-p)!}$$

ways to choose p elements from H, regarding choosing elements in different orders as different choices. However, because the order of elements in a set B does not matter, we should divide by the number of ways to arrange p elements. This is given by $p(p-1)(p-2)\cdots 3 \cdot 2 \cdot 1 = p!$ (for almost the same reason as our previous count), and so we find there are $\frac{n!}{p!(n-p)!} = \binom{n}{p}$ subsets of H with p elements.

Summing over the different possibilities for the size of a subset B, we see that there are $\sum_{p=0}^{n} \binom{n}{p}$ subsets of $\{1, 2, \dots, n\}$. □

Patrick's proof. By definition our set is $\{1, 2, \dots, n\}$. For each element in this set, we can decide either to insert it in our subset or not insert it in our subset. In creating our subset, this gives us two choices for each element of our set, up to the n-th element. Therefore, the total number of different subsets that can be created is equal to

$$\underbrace{2 \times 2 \times \ldots \times 2}_{n \text{ products}} = 2^n$$

different subsets. □

Remark 3.5. Patrick's idea is my favorite because it seems the simplest to me. It results in a very short proof. (Shorter is not always better.) Two criticisms are:

1. Patrick did not introduce the result he was proving explicitly.
2. The first use of the wording "our subset" is a little strange since the idea for the proof was not introduced.

In class, I explained the idea with an example so I decided to add this to Patrick's proof.

Michael's edit of Patrick's proof. For $n \in \mathbb{N}$, we wish to show there are 2^n subsets of $\{1, 2, \ldots, n\}$.

Our idea is to think about how to construct a subset of $\{1, 2, \ldots, n\}$ by starting with the empty set and adding elements one by one. This will allow us to count the number of decisions that we have to make to specify a subset of $\{1, 2, \ldots, n\}$. First, we might think about whether to add 1 to the subset or not. Then we might wonder whether to add 2 to the set or not. We can keep going until the last decision that we have to make: whether to add n to the set or not.

This thinking is useful because we realize that a subset A of $\{1, 2, \ldots, n\}$ is completely determined by the answer to n questions: for each $i \in \{1, 2, \ldots, n\}$, we ask "is $i \in A$?" Each question has two answers: "yes" or "no." So there are 2^n subsets of $\{1, 2, \ldots, n\}$.

It might clarify our proof further to give an example. Suppose that we are trying to determine a subset A of $\{1, 2, 3\}$. We could ask:

1. is $1 \in A$?
2. is $2 \in A$?
3. is $3 \in A$?

If the answers are "yes, no, yes," respectively, then we must have $A = \{1, 3\}$. □

4 Lecture on August 7th: $\subseteq, \cup, \cap, \setminus$, a proof

Remark 4.1. Suppose X and Y are sets, that X is a subset of Y, and that you want to write a proof for this. What do you write?

Another way of expressing the "whenever" sentence in the definition is "if $z \in X$, then $z \in Y$." To verify a sentence like "if P, then Q" directly you assume that P is true, and then check that Q is true. Thus, the definition forces our proof to look as follows.

- We wish to show $X \subseteq Y$.
- By definition, we must show that if $z \in X$, then $z \in Y$.
- So suppose that $z \in X$.
- We want to show that $z \in Y$.
- [Insert mathematical arguments to show that $z \in Y$.]
- We conclude that $z \in Y$, and so we have shown that $X \subseteq Y$.

Theorem 4.2. *Let $A = \{n \in \mathbb{N} : \ n \geq 8 \text{ and } n \text{ is prime}\}$ and $B = \{n \in \mathbb{Z} : \ n \text{ is odd}\}$.*

We have $A \subseteq B$.

Proof. Let A and B be as in the theorem statement.

We wish to show $A \subseteq B$. By definition, we must show that if $n \in A$, then $n \in B$. So suppose that $n \in A$. We want to show that $n \in B$.

Because $n \in A$, the definition of A tells us that n is a natural number which is greater than or equal 8 and prime. In order to show $n \in B$, we must demonstrate that n is an odd integer. Natural numbers are integers and n is a natural number, and so n is an integer. We are just left to show n is odd.

Suppose for contradiction that n is not odd. Then n is even, and $\frac{n}{2} \in \mathbb{N}$. Since $n \geq 8$, $\frac{n}{2} \geq 4$. Thus, writing $n = 2 \cdot \frac{n}{2}$ shows that n is not prime. This contradicts the fact that n *is* prime, and so n must be odd.

We conclude that $n \in B$, and so we have shown that $A \subseteq B$. □

Here is a complete list of the things we do during the previous proof. You might want to rewrite this list in your notes and add to it whenever we learn new things to do in a proof.

- We introduce the mathematical objects that are we are going to be using during the proof.
- We state what we wish to demonstrate before doing so.
- We unpack and use definitions where necessary (which is a lot of the time). We try to highlight when we are doing this unless we think that the reader can figure it out without such help. We should assume that the reader is another student in the class.
- We state assumptions.
- We prove an if-then statement directly.

- We use modus ponens.

  The first paragraph of `http://en.wikipedia.org/wiki/Modus_ponens` and the first paragraph of the section "explanation" are useful. You might find the rest overly confusing.

  An example of using modus ponens we might see later is: "we know convergent sequences are bounded, and (s_n) is a convergent sequence, so (s_n) is bounded."

  You could abbreviate this using the words "in particular" by saying: "(s_n) is a convergent sequence. In particular, (s_n) is bounded."

  We could also abbreviate to "since (s_n) is a convergent, (s_n) is bounded."

- We make a deduction from an assumption declared in the previous sentence.

  For example, "Suppose that (s_n) is a convergent sequence. Then (s_n) is bounded."

- We use a proof by contradiction:

  - We make an assumption that is going to cause a contradiction, the negation of what we want to verify. We use the words "suppose for contradiction..."
  - We highlight what causes the contradiction, and conclude what we wanted to verify.

- We use a mathematical equation.

- We summarize what we have done.

For each sentence of the previous proof, find the appropriate bullet point(s) describing what we are doing.

There is one case when the previous proof format for showing that $X \subseteq Y$ breaks down.

Theorem 4.3. *Suppose X is a set. Then $\emptyset \subseteq X$.*

Proof. Suppose X is a set. We wish to show that $\emptyset \subseteq X$. By definition, we must show that if $z \in \emptyset$, then $z \in X$. Since the empty set has no elements, $z \in \emptyset$ is never true, and so there is nothing to check. We conclude that $\emptyset \subseteq X$. □

Remark 4.4. Maybe the "whenever" wording makes this proof seems less strange.

Let X be a set. We must check that whenever $z \in \emptyset$, we have $z \in X$. However, since $\emptyset$ has no elements, there is nothing to check. We conclude that $\emptyset \subseteq X$.

Remark 4.5. Suppose X and Y are sets, that X is equal to Y, and that you want to write a proof for this. What do you write?

- We wish to show $X = Y$.

- By definition, we must show that $X \subseteq Y$, and $Y \subseteq X$.

- [Insert proof that $X \subseteq Y$.]

- [Insert proof that $Y \subseteq X$.]

- We have shown that $X \subseteq Y$ and $Y \subseteq X$, so we have shown that $X = Y$.

Definition 4.6. Suppose X and Y are sets.

We write $X \cup Y$ for the set

$$\{z : \ z \in X \text{ or } z \in Y\}.$$

$X \cup Y$ is read as "X *union* Y" or "the *union* of X and Y."

We write $X \cap Y$ for the set

$$\{z : \ z \in X \text{ and } z \in Y\}.$$

$X \cap Y$ is read as "X *intersect* Y" or "the *intersection* of X and Y."

We write $X \setminus Y$ for the set

$$\{z : \ z \in X \text{ and } z \notin Y\}.$$

$X \setminus Y$ is read as "X *takeaway* Y." $x \notin Y$ means, and is read as "x is not an element of Y."

Example 4.7.

1. $\{1,2\} \cup \{2,3\} = \{1,2,3\}$
2. $\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$.
3. $\{1,2\} \cap \{2,3\} = \{2\}$
4. $\{\emptyset\} \cap \{\{\emptyset\}\} = \emptyset$
5. $\{n \in \mathbb{N} : \ n \text{ is even}\} \cap \{p \in \mathbb{N} : \ p \text{ is prime}\} = \{2\}$.
6. $\{1,2,3\} \setminus \{2,3,4\} = \{1\}$.
7. $\mathbb{R} \setminus \mathbb{Q}$ is the set of irrationals.
8. $\{1,2\} \cup (\{2,3,4\} \cap \{1,3,5\}) = \{1,2,3\}$ and $(\{1,2\} \cup \{2,3,4\}) \cap \{1,3,5\} = \{1,3\}$.

5 Student proofs on August 8th

First, you'll have to read the part on $\subseteq, \cup, \cap, \setminus$.

I have explained in the lecture notes how to verify set equality. I have also explained how to verify one set is a subset of another. I wrote a proof in which I unpacked definitions. In this proof, you will certainly have to unpack the definition of $\setminus$ and $\cap$, and reference the definition of $\cup$. You should try and spell out which definitions you're using as much as possible at this early stage.

Theorem 5.1 (De Morgan's Laws)**.** *Suppose X, A, and B are sets. Then*

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B),$$

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B).$$

5.1 Making deductions using modus ponens

In class, we focussed on the first of De Morgan's laws.

I think Jean's proof taught us the most important lessons, so let's look at her proof first.

Jean's proof.

Suppose $y \in X \setminus (A \cup B)$.
If $y \in X \setminus (A \cup B)$ then it follows that $y \in X$ and $y \notin (A \cup B)$.
By definition of union $y \notin A$ and $y \notin B$.
If $y \in X$ and $y \notin A$ then $y \in X \setminus A$.
If $y \in X$ and $y \notin B$ then $y \in X \setminus B$.
If $y \in X \setminus A$ and $y \in X \setminus B$ then $y \in (X \setminus A) \cap (X \setminus B)$.
Therefore $X \setminus (A \cup B) \subseteq (X \setminus A) \cap (X \setminus B)$.

Suppose $y \in (X \setminus A) \cap (X \setminus B)$.
By definition of intersection $y \in X \setminus A$ and $y \in X \setminus B$.
If $y \in X \setminus A$ then $y \in X$ and $y \notin A$.
If $y \in X \setminus B$ then $y \in X$ and $y \notin B$.
If $y \notin A$ and $y \notin B$ then $y \notin (A \cup B)$.
Since $y \in X$ and $y \notin (A \cup B)$ it follows $y \in X \setminus (A \cup B)$.
Therefore $(X \setminus A) \cap (X \setminus B) \subseteq X \setminus (A \cup B)$.

Since both are subsets of each other, $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$. □

Remark 5.1. From reading Jean's proof, I know that she knows why De Morgan's first law is true. The proof is nice and wordy; there are not random symbols everywhere. There is an attempt at referencing relevant definitions. These are all things to celebrate!

Remark 5.2. Jean's proof is not perfect and my biggest gripe with it concerns the way in which modus ponens has been used. I'll explain this in quite some detail.

Suppose I declare that the following sentence is true:

"If I am a millionaire, then I can afford fish and chips."

You do not object. It *is* a true sentence and that is because fish and chips cost less than $\$1,000,000$. From knowing that this sentence is true, do you obtain information about whether I am a millionaire or not? No. For all you know, I could wear t-shirts with holes in to mislead you, so that you don't discover the secret fact that I am a millionaire. Do you know whether I can afford fish and chips? No again. I might be incredibly in debt, reliant on my American friend for cooking all of my meals, and every British person knows that Americans don't know how to cook fish and chips.

The point to take away is that knowing the if-then sentence above is true doesn't actually tell you very much. It describes a relationship between being a millionaire and being able to afford fish and chips. On the other hand, if, in addition, you know for certain that I am a millionaire, you can certainly conclude that I can afford fish and chips.

YOU SHOULD NOT EXPECT THE READER OF YOUR PROOF TO MAKE

SUCH A DEDUCTION. YOU ALWAYS SHOULD MAKE THE DEDUCTION FOR THEM.

There are many places in Jean's proof where she says "if P, then Q," she knows P is true, deduces Q is true *in her mind*, but does not communicate that to the reader. You saw in lecture, in real time, that this caused me to become confused. I'll go through line by line what went on in my brain as I read her proof. Bullet points 4-7 are the best examples of what I'm talking about, but I've put the others in so you know the state of my mind.

- Suppose $y \in X \setminus (A \cup B)$.

  Oh, no. Jean didn't introduce her sets. Well, let's ignore that for now.

  Okay, I have an element y in some set that I can look back on later.

- If $y \in X \setminus (A \cup B)$ then it follows that $y \in X$ and $y \notin (A \cup B)$.

  Yes, that is true by definition of $\setminus$.

- By definition of union $y \notin A$ and $y \notin B$.

  Wait, what does that have to with the definition of union?

  The definition of union involves two $\in$'s and an "or"; it doesn't involve "and."

  I guess she's done some thinking and hasn't told me everything.

  Does she know that $y \notin A \cup B$? That's not what the previous sentence says. Hmm.

  It's not what the sentence before that says either. It doesn't say this anywhere!

  Oh wait. It is a clause of an if-then sentence. Oh, I see. She used the if-then sentence, and didn't tell me that she did. The first two lines of her proof were actually: "Suppose P. If P, then Q." Why didn't she tell me to conclude Q?!?

  Then I suppose I can think for myself why $y \notin A \cup B$ means that $y \notin A$ and $y \notin B$. Ugh.

- If $y \in X$ and $y \notin A$ then $y \in X \setminus A$.

  Yes, that is true by definition of $\setminus$.

- If $y \in X$ and $y \notin B$ then $y \in X \setminus B$.

  Yes, that is true by definition of $\setminus$.

- If $y \in X \setminus A$ and $y \in X \setminus B$ then $y \in (X \setminus A) \cap (X \setminus B)$.

  Yes, that is true by definition of $\cap$.

- Therefore $X \setminus (A \cup B) \subseteq (X \setminus A) \cap (X \setminus B)$.

  Wait. What?!?!

  I don't even really remember the last three sentences because they were just some true if-then sentences. I was planning on looking them over again once Jean used them. She never told me to use them and suddenly she's claiming what I think she was trying to prove.

Many of the instances where Jean said "if P, then Q" should be replaced with "we know P is true, and that if P, then Q, so we deduce that Q is true." Admittedly this is quite long, and one way to abbreviate this is "since P is true, Q is true." In Jean's case, many of the if-then sentences follow from a definition. It is probably also best to cite which definition.

Let's fix the aspects of Jean's proof that we just discussed and no more.

Michael's partial edit of Jean's proof.

Suppose $y \in X \setminus (A \cup B)$.

It follows from the definition of $\setminus$ that $y \in X$ and $y \notin (A \cup B)$.

If y was in A, the definition of union would give $y \in A \cup B$, but this is not true, so we must have $y \notin A$.

If y was in B, the definition of union would give $y \in A \cup B$, but this is not true, so we must have $y \notin B$.

Since $y \in X$ and $y \notin A$, the definition of $\setminus$ gives $y \in X \setminus A$.

Since $y \in X$ and $y \notin B$, the definition of $\setminus$ gives $y \in X \setminus B$.

Since $y \in X \setminus A$ and $y \in X \setminus B$, the definition of $\cap$ gives $y \in (X \setminus A) \cap (X \setminus B)$.

We have now verified that if $y \in X \setminus (A \cup B)$, then $y \in (X \setminus A) \cap (X \setminus B)$,

$$\text{i.e. } X \setminus (A \cup B) \subseteq (X \setminus A) \cap (X \setminus B).$$

Suppose $y \in (X \setminus A) \cap (X \setminus B)$.

By definition of intersection, we obtain $y \in X \setminus A$ and $y \in X \setminus B$.

Since $y \in X \setminus A$, the definition of $\setminus$ gives $y \in X$ and $y \notin A$.

Since $y \in X \setminus B$, the definition of $\setminus$ gives $y \in X$ and $y \notin B$.

If y were in $A \cup B$ then the definition of union would give either $y \in A$ or $y \in B$, but we've just shown that neither of these conditions hold. Thus, we must have $y \notin (A \cup B)$.

Since $y \in X$ and $y \notin (A \cup B)$, the definition of $\setminus$ gives $y \in X \setminus (A \cup B)$.

We have now verified that if $y \in (X \setminus A) \cap (X \setminus B)$, then $y \in X \setminus (A \cup B)$,

$$\text{i.e. } (X \setminus A) \cap (X \setminus B) \subseteq X \setminus (A \cup B).$$

Since both are subsets of each other, $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$. □

5.2 Status updates

At one point in lecture I started talking about status updates.

What do I mean by status updates? Well, a mathematical statement in a proof can hold many statuses.

- It is “undeniably true.”

  I feel like three things fall into this category:

  - really easy stuff;
  - **iff** statements that are definitional;
  - theorems that you have seen the proof of, and that people reading your proof will have seen (or know where to look up quickly).

  Examples of something really easy would be the equations $0 = 0$ and $1 + 1 = 2$.

  An example of a theorem you could use is that there are 2^n subsets of $\{1, 2, \ldots, n\}$: you and your peers either know it or can look back a few pages.

  One problem with proof writing is that even the meaning of “undeniably true” warps over time. For me, it is undeniably true that $H_1(S^1) \cong \mathbb{Z}$, and I would use this in a proof for publication in a journal without hesitation. For you, you don’t even know what this means yet, so you would be very unhappy if I started using this fact over and over again in class.

  Right now, I think the main type of thing that fits in here, for you, is basic arithmetic, and basic algebra. Since we’re learning proofs, there might be some things that you thought were undeniable true, and now they need proofs. This awkward stage is unavoidable, and it’ll pass with time. And eventually more and more things will be “undeniably true” for you and your peers, as you prove more!

- It is known to be true at this stage of the proof.

  This could be for a few reasons.

  - It is an “undeniable truth.” Then it you knew it was true before the proof began, and it always will be.
  - You assumed it to be true.

    Maybe it is the premise in an if-then sentence that you are trying to verify. In that case, if you choose to verify the if-then sentence directly, you’ll suppose that it is true.

    BEWARE: the assumption might be temporary. Maybe you’ll start proving the converse if-then sentence. Then you’ll assume the other clause to be true. This is a good reason for paragraphs, and words like “conversely,” “now,” and explanations about what you’re doing.
  - You have argued it to be true based on other statements which are known to be true at this stage of the proof. If the statements which it follows from are temporarily true, it will be temporarily true too.

- You think it is true, and are trying to prove it to be true.

  You should highlight when you are starting to prove it, and when you have finished proving it.

I’m tired now and will think about adding more to this later.

6 Lecture on August 8th: Cartesian products and functions

Definition 6.1. Suppose X and Y are sets. We write $X \times Y$ for the set

$$\{(x, y) :\ x \in X,\ y \in Y\},$$

that is the set of ordered pairs where one coordinate has its value in X and the other has its value in Y. $X \times Y$ is called the *Cartesian product* of X and Y.

Definition 6.2. Suppose X is a set and $n \in \mathbb{N}$. We write X^n for the set

$$\{(x_1, x_2, \ldots, x_n) :\ x_1, x_2, \ldots, x_n \in X\}.$$

X^n is called the *n-fold Cartesian product of X*.

Example 6.3.

1. $\{0, 1\} \times \{5, 6, 7\} = \{(0, 5),\ (0, 6),\ (0, 7),\ (1, 5),\ (1, 6),\ (1, 7)\}$.

2. $\mathbb{R}^2$ is the Cartesian plane.

3. $\mathbb{R}^3$ is the home of 3D calculus.

Definition 6.4. A *function* $f : X \longrightarrow Y$ consists of:

- a set X called the *domain* of f;

- a set Y called the *codomain* of f;

- a subset G_f of the Cartesian product $X \times Y$ called the *graph of f*.

For $f : X \longrightarrow Y$ to be a function the subset $G_f \subseteq X \times Y$ must have the following properties:

- If $x \in X$, then there exists a $y \in Y$ such that $(x, y) \in G_f$.

- If $(x, y_1) \in G_f$ and $(x, y_2) \in G_f$, then $y_1 = y_2$.

When $(x, y) \in G_f$, we write $f(x) = y$.

Remark 6.5. This is the formal definition of a function $f : X \longrightarrow Y$. Normally we don't specify a subset of $X \times Y$ explicitly and instead just give a description of $f(x)$ for each $x \in X$.

The first bullet point regarding $G_f \subseteq X \times Y$ says that for every x-value there is a corresponding y value. The second bullet says that for each x-value there can only be one y-value.

Notation 6.6. We often use the notation $f : X \longrightarrow Y$, $x \longmapsto f(x)$.

"$\longmapsto$" is read as "maps to."

Example 6.7. The following are functions. Although they all have the same assignment $n \longmapsto n$, their codomains are different and so they are different functions.

1. $f : \mathbb{N} \longrightarrow \mathbb{N}$, $n \longmapsto n$.

2. $g : \mathbb{N} \longrightarrow \mathbb{Z}$, $n \longmapsto n$.

3. $h : \mathbb{N} \longrightarrow \mathbb{Q}$, $n \longmapsto n$.

4. $j : \mathbb{N} \longrightarrow \mathbb{R}$, $n \longmapsto n$.

Example 6.8. The following are functions. Although they all have the same assignment $x \longmapsto x$, their domains are different and so they are different functions.

1. $j : \mathbb{N} \longrightarrow \mathbb{R}$, $x \longmapsto x$.

2. $k : \mathbb{Z} \longrightarrow \mathbb{R}$, $x \longmapsto x$.

3. $p : \mathbb{Q} \longrightarrow \mathbb{R}$, $x \longmapsto x$.

4. $q : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto x$.

Definition 6.9. Suppose X and Y are sets and that $f : X \longrightarrow Y$ is a function.

1. We say f is *injective* **iff** whenever $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

2. We say f is *surjective* **iff** whenever $y \in Y$, we can find an $x \in X$ such that $f(x) = y$.

3. We say f is *bijective* **iff** f is injective and surjective.

Remark 6.10. We may also use "one-to-one" for injective, and "onto" for surjective.

There are noun forms of the words in the previous definition too. We speak of an injection, a surjection, and a bijection.

Remark 6.11. Suppose X and Y are sets, $f : X \longrightarrow Y$ is a function, and that f is injective.

How do you write a proof that f is injective?

Well, another way of expressing the "whenever" sentence in part 1 of the previous definition is "if $x_1, x_2 \in X$ and $f(x_1) = f(x_1)$, then $x_1 = x_2$."

Thus, the definition forces our proof to look as follows.

- We wish to show that f is injective.
- By definition, we must show that if $x_1, x_2 \in X$ and $f(x_1) = f(x_1)$, then $x_1 = x_2$.
- So suppose that $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$.
- (We want to show that $x_1 = x_2$.)
- [Insert mathematical arguments to show that $x_1 = x_2$.]
- We conclude that $x_1 = x_2$, and so we have shown that f is injective.

Kevin will talk about the following theorem a little.

Theorem 6.12. *The function* $f : \{x \in \mathbb{R} : \ x \leq 0\} \longrightarrow \mathbb{R}$, $x \longmapsto x^2$ *is injective.*

Proof. Let $X = \{x \in \mathbb{R} : \ x \leq 0\}$ and $f : X \longrightarrow \mathbb{R}$ be as in the theorem statement. We wish to show that f is injective. By definition of injectivity, we must show that if $x_1, x_2 \in X$ and $f(x_1) = f(x_1)$, then $x_1 = x_2$. So suppose $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$. By definition of f, $f(x_1) = f(x_2)$ tells us that $x_1^2 = x_2^2$. [Argue until you show that $x_1 = x_2$.] We have now shown that f is injective. □

7 Homework due on August 13th

1. Read section 5.

   Turn in your proof of De Morgan's Laws (Theorem 5.1).

2. Give the simplest examples you can to show that the following set-theoretic equations are not always true.

   (a) $(A \setminus B) \setminus C = A \setminus (B \setminus C)$.

   (b) $A \cap (B \cup C) = (A \cap B) \cup C$.

3. In this question, the correct number is good enough for full credit.

   Leaving numbers in a form that shows your thinking is best though.

   (a) How many functions are there with domain $\{1, 2, 3\}$ and codomain $\{1, 2, 3, 4, 5\}$?

   (b) How many injective functions are there with domain $\{1, 2, 3\}$ and codomain $\{1, 2, 3, 4, 5\}$?

   (c) How many surjective functions are there with domain $\{1, 2, 3\}$ and codomain $\{1, 2, 3, 4, 5\}$?

   (d) How many functions are there with domain $\{1, 2, 3, 4, 5\}$ and codomain $\{1, 2, 3\}$?

   (e) How many injective functions are there with domain $\{1, 2, 3, 4, 5\}$ and codomain $\{1, 2, 3\}$?

   (f) How many surjective functions are there with domain $\{1, 2, 3, 4, 5\}$ and codomain $\{1, 2, 3\}$? Hint: how many functions are there with domain $\{1, 2, 3, 4, 5\}$ and codomain $\{1, 2\}$?

   (g) Let $n \in \mathbb{N}$. How many bijections are there with domain and codomain $\{1, 2, \ldots, n\}$?

4. (a) **Theorem 7.1.** *The function* $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ *defined by* $h(m, n) = 2^{m-1}(2n - 1)$ *is an injection.*

   (b) In fact, h is surjective too. I might not have shown you a surjective proof by this point. If you want to try and prove this, go for it. This question won't be graded yet, but will probably be on the next homework.

5. (a) **Theorem 7.2.** *Let* $n \in \mathbb{N}$. *The function* $b : \{0, 1\}^n \longrightarrow \{0, 1, 2, \ldots, 2^n - 1\}$ *defined by*

   $$b(x_0, x_1, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} x_i \cdot 2^i$$

   is injective.

   I give some hints to help you prove this in the next section.

   (b) Is the function of the theorem a bijection? Give a quick reason for your answer.

6. (a) Define a surjection $j : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Q}$. You don't need to prove it is a surjection.

   (b) Define a bijection $k : \mathbb{N} \longrightarrow \mathbb{Z}$. You don't need to prove it is a bijection, but you should define your function without using ellipses (that is don't use ...s).

8 Hints for proving theorem 9.3

This is quite a tricky theorem to prove. I should give some hints so that you gain more from doing this question…

1. To prove b is injective it is enough to show that

   - if $(x_0, x_1, \ldots, x_{n-1}), (y_0, y_1, \ldots, y_{n-1}) \in \{0,1\}^n$ and
   $$(x_0, x_1, \ldots, x_{n-1}) \neq (y_0, y_1, \ldots, y_{n-1}),$$
   then $b(x_0, x_1, \ldots, x_{n-1}) \neq b(y_0, y_1, \ldots, y_{n-1})$.

   Do you agree? Why is this? How does this statement relate to the definition of injective?

2. Suppose the premise of the if-then sentence above and let m be the largest i such that $x_i \neq y_i$.

   To argue that $b(x_0, x_1, \ldots, x_{n-1}) \neq b(y_0, y_1, \ldots, y_{n-1})$, it is enough to show that
   $$b(x_0, x_1, \ldots, x_{n-1}) < b(y_0, y_1, \ldots, y_{n-1}) \text{ or } b(x_0, x_1, \ldots, x_{n-1}) > b(y_0, y_1, \ldots, y_{n-1}).$$

3. To work towards either of the inequalities just mentioned, you might find it useful to use the trivial fact that 0 and 1 are both less than or equal to 1. You may also find it useful to use the less trivial fact that for $a \in \mathbb{R}$, $r \in \mathbb{R} \setminus \{1\}$, and $M \in \mathbb{N}$,
   $$\sum_{i=0}^{M-1} a \cdot r^i = \frac{a(1 - r^M)}{1 - r}.$$

   Think about what this says when $a = 1$ and $r = 2$.

   You can use the less trivial fact without proof, and I will happily prove this to you if you do not know a proof.

4. If you are not understanding the hint in part 3, take $n = 5$ and think about why
   $$b(1,0,1,0,0) \leq b(1,1,1,0,0) < b(0,0,0,1,0) \leq b(1,1,0,1,0).$$

   How does this help you show $b(1,0,1,0,1) < b(1,1,0,1,1)$?

9 Solutions to homework 1

1. Suppose X, A, and B are sets. We wish to show that

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B).$$

By definition of set equality, we must show that

$$X \setminus (A \cup B) \subseteq (X \setminus A) \cap (X \setminus B) \quad \text{and} \quad X \setminus (A \cup B) \supseteq (X \setminus A) \cap (X \setminus B).$$

(a) First, we demonstrate that $X \setminus (A \cup B) \subseteq (X \setminus A) \cap (X \setminus B)$.

By definition of $\subseteq$, we have to show that whenever $z \in X \setminus (A \cup B)$, it is the case that $z \in (X \setminus A) \cap (X \setminus B)$.

So suppose $z \in X \setminus (A \cup B)$. By definition of $\setminus$, this means $z \in X$ and $z \notin A \cup B$. We cannot have $z \in A$ or $z \in B$ since, by the definition of $\cup$, both these conditions imply $z \in A \cup B$.

Thus, $z \in X$ and $z \notin A$, and the definition of $\setminus$ gives $z \in X \setminus A$.

Similarly, $z \in X$ and $z \notin B$, and the definition of $\setminus$ gives $z \in X \setminus B$.

By the definition of $\cap$, the last two facts say $z \in (X \setminus A) \cap (X \setminus B)$.

(b) Next, we show that $X \setminus (A \cup B) \supseteq (X \setminus A) \cap (X \setminus B)$, i.e if $z \in (X \setminus A) \cap (X \setminus B)$, then $z \in X \setminus (A \cup B)$.

Suppose that $z \in (X \setminus A) \cap (X \setminus B)$. By definition of $\cap$, this means that $z \in X \setminus A$ and $z \in X \setminus B$.

The first statement together with the definition of $\setminus$ says $z \in X$ and $z \notin A$.

The second statement together with the definition of $\setminus$ says $z \in X$ and $z \notin B$.

If we had $z \in A \cup B$, by definition of $\cup$, we'd have either $z \in A$ or $z \in B$, and this is not the case. Thus, $z \notin A \cup B$.

In conclusion, $z \in X$ and $z \notin A \cup B$, so the definition of $\setminus$ gives $z \in X \setminus (A \cup B)$.

Suppose X, A, and B are sets. We wish to show that

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B).$$

By definition of set equality, we must show that

$$X \setminus (A \cap B) \subseteq (X \setminus A) \cup (X \setminus B) \quad \text{and} \quad X \setminus (A \cap B) \supseteq (X \setminus A) \cup (X \setminus B).$$

(a) First, we demonstrate that $X \setminus (A \cap B) \subseteq (X \setminus A) \cup (X \setminus B)$, that is, if $z \in X \setminus (A \cap B)$, then $z \in (X \setminus A) \cup (X \setminus B)$.
Suppose $z \in X \setminus (A \cap B)$. By definition of $\setminus$, this means $z \in X$ and $z \notin A \cap B$.
We cannot have both $x \in A$ and $x \in B$ since, by definition of $\cap$, this would tell us that $z \in A \cap B$.

   i. Case 1: $z \notin A$. Since $z \in X$, the definition of $\setminus$ tells us that $z \in X \setminus A$.
   Thus, by definition of $\cup$, $z \in (X \setminus A) \cup (X \setminus B)$.

   ii. Case 2: $z \notin B$. Since $z \in X$, the definition of $\setminus$ tells us that $z \in X \setminus B$.
   Thus, by definition of $\cup$, $z \in (X \setminus A) \cup (X \setminus B)$.

In either case we have shown that $z \in (X \setminus A) \cup (X \setminus B)$.

(b) Next, we show that if $z \in (X \setminus A) \cup (X \setminus B)$, then $z \in X \setminus (A \cap B)$.
Suppose $z \in (X \setminus A) \cup (X \setminus B)$. By definition of $\cup$, this means $z \in X \setminus A$ or $z \in X \setminus B$.

   i. Case 1: $z \in X \setminus A$. By definition of $\setminus$, this means that $z \in X$ and $z \notin A$.
   We cannot have $z \in A \cap B$, since otherwise, by the definition of $\cap$, we'd have $z \in A$.
   So $z \in X$ and $z \notin A \cap B$, and the definition of $\setminus$ gives $z \in X \setminus (A \cap B)$.

   ii. Case 2: $z \in X \setminus B$. By definition of $\setminus$, this means that $z \in X$ and $z \notin B$.
   We cannot have $z \in A \cap B$, since otherwise, by the definition of $\cap$, we'd have $z \in B$.
   So $z \in X$ and $z \notin A \cap B$, and the definition of $\setminus$ gives $z \in X \setminus (A \cap B)$.

In either case we have shown that $z \in X \setminus (A \cap B)$.

2. (a) $(\{1\} \setminus \{1\}) \setminus \{1\} = \emptyset \setminus \{1\} = \emptyset \neq \{1\} = \{1\} \setminus \emptyset = \{1\} \setminus (\{1\} \setminus \{1\})$.
   (b) $\emptyset \cap (\emptyset \cup \{1\}) = \emptyset \neq \{1\} = \emptyset \cup \{1\} = (\emptyset \cap \emptyset) \cup \{1\}$.

3. (a) 5^3.

   (b) $5 \cdot 4 \cdot 3$.

   (c) 0.

   (d) 3^5.

   (e) 0.

   (f) Let try to count how many functions $f : \{1, 2, 3, 4, 5\} \longrightarrow \{1, 2, 3\}$ are NOT surjective. There are three cases: Let $X = \{1, 2, 3, 4, 5\}$

      i. $1 \notin f(A)$: then f is basically a function $X \longrightarrow \{2, 3\}$. There are 2^5 such functions.

      ii. $2 \notin f(A)$: then f is basically a function $X \longrightarrow \{1, 3\}$. There are 2^5 such functions.

      iii. $3 \notin f(A)$: then f is basically a function $X \longrightarrow \{1, 2\}$. There are 2^5 such functions.

   It looks like we have counted that there are $3 \cdot 2^5$ functions which are NOT surjective. But we have double counted: there are three constant functions which have been counted twice. So there are $3 \cdot 2^5 - 3$ functions which are NOT sujective.

   The answer is $3^5 - 3 \cdot 2^5 + 3$.

   (g) $n!$

4. (a) **Theorem 9.1.** *The function $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ defined by $h(m, n) = 2^{m-1}(2n - 1)$ is an injection.*

   Proof. Let $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ be defined by $h(m, n) = 2^{m-1}(2n - 1)$.

   We wish to show that h is injective.

   So let $(m_1, n_1), (m_2, n_2) \in \mathbb{N} \times \mathbb{N}$ and suppose that $h(m_1, n_1) = h(m_2, n_2)$.

   We wish to show that $(m_1, n_1) = (m_2, n_2)$ which is the same as $m_1 = m_2$ and $n_1 = n_2$.

   By definition of h, $h(m_1, n_1) = h(m_2, n_2)$ tells us that

$$2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1). \tag{9.2}$$

   By dividing (9.2) by 2^{m_2-1}, we obtain

$$2^{m_1-m_2}(2n_1 - 1) = 2n_2 - 1.$$

   The right-hand side is an odd integer, and so the left-hand side must be an odd integer too. We cannot have $m_1 - m_2 > 0$ because this would imply the left-hand side is even. Thus, we have $m_1 - m_2 \leq 0$.

   By dividing (9.2) by 2^{m_1-1}, we obtain

$$2n_1 - 1 = 2^{m_2-m_1}(2n_2 - 1).$$

   The left-hand side is an odd integer, and so the right-hand side must be an odd integer too. We cannot have $m_2 - m_1 > 0$ because this would imply the right-hand side is even. Thus, we have $m_2 - m_1 \leq 0$.

   We have shown that $m_1 - m_2 \leq 0$ and $m_2 - m_1 \leq 0$. Thus, $m_1 = m_2$.

   From (9.2) and $m_1 = m_2$, we obtain $2n_1 - 1 = 2n_2 - 1$, and so $n_1 = n_2$.

   We've shown that $(m_1, n_1) = (m_2, n_2)$ and so we have demonstrated that h is injective. □

(b) Omitted, since it is on the next homework.

5. (a) **Theorem 9.3.** *Let $n \in \mathbb{N}$. The function $b : \{0,1\}^n \longrightarrow \{0,1,2,\ldots,2^n-1\}$ defined by*

$$b(x_0, x_1, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} x_i \cdot 2^i$$

is injective.

Proof. Let $n \in \mathbb{N}$ and $b : \{0,1\}^n \longrightarrow \{0,1,2,\ldots,2^n-1\}$ be as in the theorem statement. We wish to show that b is injective. So let $(x_0, x_1, \ldots, x_{n-1}), (y_0, y_1, \ldots, y_{n-1}) \in \{0,1\}^n$ and suppose that $(x_0, x_1, \ldots, x_{n-1}) \neq (y_0, y_1, \ldots, y_{n-1})$. We wish to show that

$$b(x_0, x_1, \ldots, x_{n-1}) \neq b(y_0, y_1, \ldots, y_{n-1}).$$

Let m be the largest $i \in \{0, 1, \ldots, n-1\}$ such that $x_i \neq y_i$. There are two cases:

i. $x_m = 0$ and $y_m = 1$. Then

$$\sum_{i=0}^{m} x_i \cdot 2^i = \sum_{i=0}^{m-1} x_i \cdot 2^i \leq \sum_{i=0}^{m-1} 2^i = 2^m - 1 < 2^m \leq \sum_{i=0}^{m} y_i \cdot 2^i. \tag{9.4}$$

Here, the first equality is true because $x_m = 0$; the second inequality uses the fact that each $x_i \leq 1$; the equality follows from the formula for a geometric sum; and the last inequality follows from the fact that each $y_i \geq 0$ and $y_m = 1$.
Since m is the *largest* $i \in \{0, 1, \ldots, n-1\}$ with $x_i \neq y_i$, we have

$$\sum_{i=m+1}^{n-1} x_i \cdot 2^i = \sum_{i=m+1}^{n-1} y_i \cdot 2^i.$$

By adding this expression to both sides of (9.4), we obtain

$$b(x_0, x_1, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} x_i \cdot 2^i < \sum_{i=0}^{n-1} y_i \cdot 2^i = b(y_0, y_1, \ldots, y_{n-1}).$$

ii. $x_m = 1$ and $y_m = 0$. Identically to above, but with the roles of x and y swapped, we can show that $b(x_0, x_1, \ldots, x_{n-1}) > b(y_0, y_1, \ldots, y_{n-1})$.

In both cases, we have shown that $b(x_0, x_1, \ldots, x_{n-1}) \neq b(y_0, y_1, \ldots, y_{n-1})$. Thus, b is injective. □

(b) b is bijective!
Note that $\{0,1\}^n$ has 2^n elements, and that $\{0,1,2,\ldots,2^n-1\}$ also has 2^n elements.
If b were not surjective, it would take 2^n elements to strictly less than 2^n elements, and the pigeonhole principle would tell us b is not injective. However, we know b is injective. Thus, b must also be surjective.
`http://en.wikipedia.org/wiki/Pigeonhole_principle`

6. (a) Define $j : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Q}$ by $(m, n) \longmapsto \frac{m}{n}$.

(b) Define $k : \mathbb{N} \longrightarrow \mathbb{Z}$. By

$$k(n) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd;} \\ -\frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

10 Student proofs on August 13th

Theorem 9.1.

Note that I have changed this. Previously, I was planning for you to prove theorem 9.3 in class. Kevin and I decided that theorem 9.3 is a bit too tricky for presenting. Moreover, theorem 9.1 is probably more important for understanding the significance of Cantor's result.

Leah's proof. Function $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ defined by $h(m,n) = 2^{m-1}(2n-1)$ is an injection.

Proof. Let h be a function defined by the above statement. Let us define m_1, m_2, n_1, n_2 to be arbitrary elements of $\mathbb{N} \times \mathbb{N}$. Assume for injective functions that $f(x_1) = f(x_2)$. If we plug m_1 and n_1 into h then we get $h(m_1, n_1) = 2^{m_1-1}(2n_1-1)$. We must find that $m_1 = m_2$.

$$h(m_1, n_1) = h(m_2, n_2)$$

$$2^{m_1-1}(2n_1-1) = 2^{m_2-1}(2n_2-1)$$

$$2^{\frac{m_1}{m_2}}(2n_1-1) = 2^0(2n_2-1)$$

$$2^{m_1-m_2}(2n_1-1) = 2^0(2n_2-1)$$

$$m_1 - m_2 = 0$$

$$m_1 = m_2$$

Therefore, we have shown that h is an injective function. □

Remark 10.1. We can see some good arguments in this proof. But some things are said incorrectly.

1. "Let h be *a* function defined by..." There is only one such function, so it is better to say, "let h be *the* function defined by..."

2. m_1, m_2, n_1, n_2 are not elements of $\mathbb{N} \times \mathbb{N}$, and Leah's not really defining them. Better to say, "Let $(m_1, n_1), (m_2, n_2)$ be arbitrary elements of $\mathbb{N} \times \mathbb{N}$."

3. "Assume for injective functions that $f(x_1) = f(x_2)$." What is f? What is x_1, x_2? What does "assume for injective functions" mean?

4. "We must find $m_1 = m_2$." That's only half of what needs to be done. In order to show that $(m_1, n_1) = (m_2, n_2)$, we need to show both $m_1 = m_2$ *and* $n_1 = n_2$.

5. The list of equations looks like scratch work. Is one equation being deduced from the former? Use, at the very least, the word "so" if this is what is happening.

6. $2^{\frac{m_1}{m_2}} \neq 2^{m_1-m_2}$. The third equation needs to be scribbled out ASAP!

Jessica's proof. The function $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ defined by $h(m, n) = 2^{m-1}(2n-1)$ is an injection. By definition of injectivity, we must show that $(m_1, n_1), (m_2, n_2) \in \mathbb{N} \times \mathbb{N}$ and $h(m_1, n_1) = h(m_2, n_2)$, then $(m_1, n_1) = (m_2, n_2)$.

Suppose $h(m_1, n_1) = h(m_2, n_2)$ then we need to show $(m_1, n_1) = (m_2, n_2)$.

By definition of h, $h(m_1, n_1) = h(m_2, n_2)$ tells us that

$$\frac{2^{m_1-1}(2n_1-1)}{2^{m_2-1}} = \frac{2^{m_2-1}}{2^{m_2-1}}(2n_2-1) \implies 2^{m_1-m_2}(2n_1-1) = (2n_2-1)$$

To cancel out $2^{m_1-m_2}$, $m_1 - m_2 = 0$. $2^0(2n_1-1) = (2n_2-1)$. $n_1 = n_2$.

Therefore, $(m_1, n_1) = (m_2, n_2)$. We have shown h is injective. □

Remark 10.2. The set up of this proof is very good. The most important idea in the proof is not highlighted, but, since we'll see that in Von's proof, let's focus on the start.

1. The first sentence reads like an assertion. It's actually the theorem statement. Inserting the words "we want to show" would be a good idea.

2. In the next sentence there is a beautiful comma together with the word "then," but the word "if" is missing! Maybe this was Jessica copying off of her paper incorrectly.

3. "Suppose $h(m_1, n_1) = h(m_2, n_2)$ then we need to show $(m_1, n_1) = (m_2, n_2)$" would be better as "Suppose $(m_1, n_1), (m_2, n_2) \in \mathbb{N} \times \mathbb{N}$ and $h(m_1, n_1) = h(m_2, n_2)$. We need to show $(m_1, n_1) = (m_2, n_2)$."

4. Other than these minor adjustments the set up is perfect. I drew a heart < 3.

More major issues were:

1. "By definition of h, $h(m_1, n_1) = h(m_2, n_2)$ tells us that

   $$\frac{2^{m_1-1}(2n_1-1)}{2^{m_2-1}} = \frac{2^{m_2-1}}{2^{m_2-1}}(2n_2-1) \implies 2^{m_1-m_2}(2n_1-1) = (2n_2-1)\text{''}$$

   would be said in words as "By definition of h, $h(m_1, n_1) = h(m_2, n_2)$ tells us that if BLAH, then BLAH." I don't think the definition of h has anything to do with an if-then sentence. The point I'm making here is that "$\implies$" has been misused.

2. Also, Jessica had crossed out $\frac{2^{m_2-1}}{2^{m_2-1}}$. This type of cancellation should almost never appear in a math proof. It means more than one step happened. It looks too much like scratch work.

3. I would address the first two points by writing the following instead...

   By definition of h, $h(m_1, n_1) = h(m_2, n_2)$ tells us that $2^{m_1-1}(2n_1-1) = 2^{m_2-1}(2n_2-1)$.

   Dividing by 2^{m_2-1} gives $2^{m_1-m_2}(2n_1-1) = 2n_2 - 1$.

4. "To cancel out $2^{m_1-m_2}$, $m_1 - m_2 = 0$."

   This is the crux of the proof and it is not explained well enough. Let's move onto Von's proof.

Von's proof. The function $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ defined by $h(m, n) = 2^{m-1}(2n - 1)$ is an injection.

Proof. Let $m_1, m_2, n_1, n_2 \in \mathbb{N}$ and $h(m_1, n_1) = h(m_2, n_2)$. To satisfy the definition of an injective function in the given case, we must show that $m_1 = m_2$ and $n_1 = n_2$.

We've assumed $2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1) \iff 2^{m_1-m_2}(2n_1 - 1) = (2n_2 - 1)$.

Without loss of generality, assume $m_1 > m_2$. Therefore, since $m_1, m_2 \in \mathbb{N}$, we have $m_1 - m_2 \in \{1, 2, 3, \dots, k\}$. Notice this makes $2^{m_1-m_2}(2n_1-1)$ an <u>even</u> number. But for any choice of $n_1, n_2 \in \mathbb{N}$, $(2n_2 - 1)$ is an <u>odd</u> number. So the assumption that $m_1 > m_2$ produces a contradiction. Therefore, it must be that $m_1 = m_2$.

Now we must show that $n_1 = n_2$. Since $m_1 = m_2$, we get

$$2^0(2m_1 - 1) = (2m_2 - 1) \iff 2n_1 - 1 = 2n_2 - 1 \iff n_1 = n_2.$$

Since both $n_1 = n_2$ and $m_1 = m_2$, function h is an injection. □

Remark 10.3. Von's proof highlights the reason the theorem is true very clearly. Working under a false premise (for the sake of contradiction), he says, "Notice this makes $2^{m_1-m_2}(2n_1 - 1)$ an <u>even</u> number. But for any choice of $n_2 \in \mathbb{N}$, $(2n_2 - 1)$ is an <u>odd</u> number." The other proofs said nothing about odd or even numbers.

I'll omit saying everything I said in class, and focus on two critcisms I have of Von's proof.

1. The first is minor and is a mistake very similar to one I have already pointed out in Jessica's proof: he misuses " $\iff$."

   He says, "We've assumed $2^{m_1-1}(2n_1-1) = 2^{m_2-1}(2n_2-1) \iff 2^{m_1-m_2}(2n_1-1) = (2n_2-1)$." We never assumed "$2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1)$ is equivalent to $2^{m_1-m_2}(2n_1 - 1) = (2n_2 - 1)$." This is true because the math-gods made it true!

   What he meant to say was, "We've assumed $2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1)$, and this is equivalent to $2^{m_1-m_2}(2n_1 - 1) = (2n_2 - 1)$.

2. The second concerns "without loss of generality," and the fact he is actually doing a proof by contradiction which was not introduced.

   By the fourth line, part of his goal is to show $m_1 = m_2$. So assuming that $m_1 > m_2$ sounds like a ridiculous idea. I'd change his proof to say the following...

   Suppose for contradiction that $m_1 > m_2$. Since $m_1, m_2 \in \mathbb{N}$, this assumption gives $m_1 - m_2 \in \mathbb{N}$. Notice that this makes $2^{m_1-m_2}(2n_1 - 1)$ an <u>even</u> number. But for any choice of $n_2 \in \mathbb{N}$, $2n_2 - 1$ is an <u>odd</u> number. This contradicts that fact that $2^{m_1-m_2}(2n_1 - 1) = 2n_2 - 1$. So the assumption that $m_1 > m_2$ produces a contradiction. Therefore, it must be that $m_1 \leq m_2$.

   He should then add an argument for $m_1 \geq m_2$. Alternatively, he could have said "Suppose without loss of generality that $m_1 \geq m_2$. Suppose for contradiction that $m_1 > m_2$. [Same as before.] Therefore it must be that $m_1 = m_2$."

My proof. We wish to show that $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ defined by $h(m,n) = 2^{m-1}(2n-1)$ is injective.

So let $(m_1, n_1), (m_2, n_2) \in \mathbb{N} \times \mathbb{N}$ and suppose that $h(m_1, n_1) = h(m_2, n_2)$.

We wish to show that $(m_1, n_1) = (m_2, n_2)$ which is the same as $m_1 = m_2$ and $n_1 = n_2$.

By definition of h, $h(m_1, n_1) = h(m_2, n_2)$ tells us that

$$2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1). \tag{10.4}$$

By dividing (10.4) by 2^{m_2-1}, we obtain

$$2^{m_1-m_2}(2n_1 - 1) = 2n_2 - 1.$$

The right-hand side is an odd integer, and so the left-hand side must be an odd integer too. We cannot have $m_1 - m_2 > 0$ because this would imply the left-hand side is an even integer. Thus, we have $m_1 - m_2 \leq 0$.

By dividing (10.4) by 2^{m_1-1}, we obtain

$$2n_1 - 1 = 2^{m_2-m_1}(2n_2 - 1).$$

The left-hand side is an odd integer, and so the right-hand side must be an odd integer too. We cannot have $m_2 - m_1 > 0$ because this would imply the right-hand side is an even integer. Thus, we have $m_2 - m_1 \leq 0$.

We have shown that $m_1 - m_2 \leq 0$ and $m_2 - m_1 \leq 0$. Thus, $m_1 = m_2$.

From (10.4) and $m_1 = m_2$, we obtain $2n_1 - 1 = 2n_2 - 1$, and so $n_1 = n_2$.

We've shown that $(m_1, n_1) = (m_2, n_2)$ and so we have demonstrated that h is injective. □

Remark 10.5. Finally, I made some remarks concerning "forwards" proofs, "backwards" proofs, and "meeting in the middle" proofs.

Suppose that you want to prove a statement "if P, then S." Perhaps the reason this is true is because each of the following statements is true.

1. If P, then Q;
2. If Q, then R;
3. If R, then S.

If each of the these if-then sentences are known or obvious, then you would probably write a "forwards" proof. "Suppose P. Since P, we have Q. Since Q, we have R. Since R, we have S and this completes the proof of if P, then S."

You could also write a "backwards" proof. "Suppose P. We want to show S. If R, then S, and so it is enough to show R. If Q, then R, and so it is enough to show Q. If P, then Q, and so it is enough to show P. We assumed P, so we're done."

Normally when writing proofs, I try to save the hardest part until last. Perhaps the middle if-then is much harder to justify. Then you might try a "meeting in the middle" proof. "Suppose P. Since P, we have Q. We want to show S. If R, then S, and so it is enough to show R. To finish the proof, we just have to argue that if Q, then R. [Then focus only on this final difficult if-then sentence.]"

This comment relates to status updates. As long as you indicate carefully what is known to be true versus what you are tryng to show is true, you can basically do whatever you want.

11 Lecture on August 13th and August 15th

11.1 Functions (cont'd)

Recall definition 6.9.

Definition. Suppose X and Y are sets and that $f : X \longrightarrow Y$ is a function.

1. We say f is *injective* **iff** whenever $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$.
2. We say f is *surjective* **iff** whenever $y \in Y$, we can find an $x \in X$ such that $f(x) = y$.
3. We say f is *bijective* **iff** f is injective and surjective.

Remark 11.1.1. Suppose X and Y are sets, $f : X \longrightarrow Y$ is a function, and that f is surjective.

How do you write a proof that f is surjective?

Well, another way of expressing the "whenever" sentence in part 2 of the previous definition is "if $y \in Y$, then we can find an $x \in X$ such that $f(x) = y$."

Thus, the definition forces our proof to look as follows.

- We wish to show that f is surjective.
- By definition, we must show that if $y \in Y$, then we can find an $x \in X$ such that $f(x) = y$.
- So suppose that $y \in Y$.
- (We want to show that we can find an $x \in X$ such that $f(x) = y$.)
- [Insert mathematical arguments.]

  These arguments must do two things:

  - Specify an element $x \in X$.
  - Check that the specified x satisfies the equation $f(x) = y$.
- We have completed the demonstration that f is surjective.

Theorem 11.1.2. *The function $f : \mathbb{R} \longrightarrow \{y \in \mathbb{R} : \ y \geq 0\}$, $x \longmapsto x^2$ is surjective.*

Proof. Let $Y = \{y \in \mathbb{R} : \ y \geq 0\}$ and $f : \mathbb{R} \longrightarrow Y$ be defined as in the theorem statement. We wish to show that f is surjective. By definition of surjectivity, we must show that if $y \in Y$, then we can find an $x \in \mathbb{R}$ such that $f(x) = y$. So suppose that $y \in Y$. Since $y \geq 0$, we can let $x = \sqrt{y}$. Then $f(x) = x^2 = (\sqrt{y})^2 = y$, and we have completed the demonstration that f is surjective. □

Remark 11.1.3. This proof requires using the square root function. How do we know such a function exists? In a class on real analysis you would prove such a function exists by using the intermediate value theorem.

Theorem 11.1.4. *The function $f : \{x \in \mathbb{R} : \ x \geq 0\} \longrightarrow \{y \in \mathbb{R} : \ y \geq 0\}$, $x \longmapsto x^2$ is a bijection.*

Proof. Omitted. □

11.2 Bijections and inverse functions

Definition 11.2.1. Suppose X, Y, and Z are sets, and that $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ are functions. The *composition of f and g* is the function $g \circ f : X \to Z$ defined by $(g \circ f)(x) = g(f(x))$.

Definition 11.2.2. Suppose X is a set. The *identity* function on X is the function

$$1_X : X \longrightarrow X,\ x \longmapsto x.$$

Definition 11.2.3. Suppose X and Y are sets and $f : X \longrightarrow Y$ is a function.

f is said to be *invertible* **iff** there exists a function $g : Y \longrightarrow X$ such that

$$g \circ f = 1_X \text{ and } f \circ g = 1_Y.$$

Theorem 11.2.4. *A function $f : X \longrightarrow Y$ is invertible if and only if it is bijective.*

Proof. "**Only if.**"

Suppose $f : X \longrightarrow Y$ is invertible. We must show that f is bijective.

Choose $g : Y \longrightarrow X$ such that $g \circ f = 1_X$ and $f \circ g = 1_Y$.

First, we show that f is injective. Let $x_1, x_2 \in X$. Suppose that $f(x_1) = f(x_2)$. Then

$$x_1 = 1_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = 1_X(x_2) = x_2.$$

Next, we show that f is surjective. Let $y \in Y$. Let $x = g(y)$. Then

$$f(x) = f(g(y)) = (f \circ g)(y) = 1_Y(y) = y.$$

"**If.**"

Suppose that f is a bijection. We must show that f is invertible. We need to define a function $g : Y \longrightarrow X$. We define it via its graph.

$$G_g = \{(y, x) \in Y \times X : \ (x, y) \in G_f\}.$$

For $g : Y \longrightarrow X$ to be a function the subset G_g must have the following properties:

- If $y \in Y$, then there exists an $x \in X$ such that $(y, x) \in G_g$.
- If $(y, x_1) \in G_g$ and $(y, x_2) \in G_g$, then $x_1 = x_2$.

By using the definition of G_g, we see that these are the same as asking for:

- If $y \in Y$, then there exists an $x \in X$ such that $(x, y) \in G_f$.
- If $(x_1, y) \in G_f$ and $(x_2, y) \in G_f$, then $x_1 = x_2$.

Using more standard notation, we see that these are the same as asking for:

- If $y \in Y$, then there exists an $x \in X$ such that $f(x) = y$.
- If $f(x_1) = y$ and $f(x_2) = y$, then $x_1 = x_2$.

The first is the true because f is surjective. The second is true because f is injective.

Our graph definition says that for all $x \in X$ and $y \in Y$,

$$g(y) = x \text{ if and only if } f(x) = y.$$

Let $x \in X$. Since $f(x) = f(x)$, we obtain $g(f(x)) = x$.

Let $y \in Y$. Since $g(y) = g(y)$, we obtain $f(g(y)) = y$.

These two statements say that $g \circ f = 1_X$ and $f \circ g = 1_Y$. □

11.3 Cardinality

Definition 11.3.1. Let X be a set.

1. We say X is *finite* **iff** $X = \emptyset$ or we can find an $n \in \mathbb{N}$ and a bijection $f : \{1, 2, \ldots, n\} \longrightarrow X$.
2. We say X is *infinite* **iff** X is not finite.

Definition 11.3.2. Let X be a set.

1. We say X is *countable* **iff** $X = \emptyset$ or there exists a surjection $f : \mathbb{N} \longrightarrow X$.
2. We say X is *uncountable* **iff** X is not countable.

Theorem 11.3.3. *Finite sets are countable.*

Proof. Suppose X is a finite set. We must show X is countable.

If $X = \emptyset$, then we immediately see that X is countable, so assume $X \neq \emptyset$.

By definition of a set being finite, we can find an $n \in \mathbb{N}$ and a bijection $f : \{1, 2, \ldots, n\} \longrightarrow X$.

Define $g : \mathbb{N} \longrightarrow \{1, 2, \ldots, n\}$ by $g(k) = \min\{k, n\}$.

Notice that for all $k \in \{1, 2, \ldots, n\}$, we have $g(k) = k$, so g is surjective.

The function $f \circ g : \mathbb{N} \longrightarrow X$ is the composition of two surjective functions.

By one of your assignments, this shows that $f \circ g$ is surjective. So X is countable. □

Definition 11.3.4. We say X is *countably infinite* **iff** X is countable and infinite.

Example 11.3.5. $\mathbb{N}$ is countably infinite. It is clearly infinite. Moreover, we can take the identity map $1_{\mathbb{N}} : \mathbb{N} \longrightarrow \mathbb{N}$ as the required surjection.

Example 11.3.6. $\mathbb{Q}$ is also countably infinite. You'll prove this at the end of the week.

Definition 11.3.7. Let X and Y be sets.

We say that X and Y have the same *cardinality* **iff** there exists a bijection $f : X \longrightarrow Y$.

Remark 11.3.8. Notice that there is a bijection $X \longrightarrow Y$ if and only there is a bijection $Y \longrightarrow X$ because we can use theorem 11.2.4: if a function $X \longrightarrow Y$ is a bijection, it has an inverse $Y \longrightarrow X$ and this is a bijection too.

Definition 11.3.9. Suppose X is a set. The *powerset of* X is the set $\{A : A \subseteq X\}$.

Example 11.3.10. $\mathcal{P}(\{1, 2\}) = \Bigg\{\emptyset, \{1\}, \{2\}, \{1, 2\}\Bigg\}$.

Example 11.3.11. We have seen that for $n \in \mathbb{N}$, $\mathcal{P}(\{1, 2, \ldots, n\})$ has 2^n elements.

Theorem 11.3.12 (Cantor)**.** *Let X be a set. Then X and $\mathcal{P}(X)$ do not have the same cardinality.*

Remark 11.3.13. For any set X, there is an "obvious" injection

$$X \longrightarrow \mathcal{P}(X), \ x \longmapsto \{x\}.$$

This shows $\mathcal{P}(X)$ is at least as big as X. The fact that X and $\mathcal{P}(X)$ do not have the same cardinality means $\mathcal{P}(X)$ is *strictly* larger in size than X.

12 Student proofs on August 15th

Theorem 12.1. *Suppose X, Y, and Z are sets, and $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ are functions.*

1. *If $g \circ f$ is injective, then f is injective.*
2. *If $g \circ f$ is surjective, then g is surjective.*
3. *If f and g are injective, then $g \circ f$ is injective.*
4. *If f and g are surjective, then $g \circ f$ is surjective.*

I'll just ask to see part 1 and 4.

A very good job was done of this. I'll try to post something.

13 Student proofs on August 16th

Theorem 13.1. $\mathbb{Q}$ *is countable.*

If you google this, you'll almost certainly find a picture proof. It is good to understand that proof, but I would like you to define an explicit surjection. For me, "explicit" includes the composition of explicitly defined functions and their inverses.

Some things to note...

1. You have already defined a surjection $j : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Q}$ and a bijection $k : \mathbb{N} \longrightarrow \mathbb{Z}$. You will prove that they are a surjection and bijection, respectively, on the next homework. You can assume this for now.
2. I defined a map $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$. You have proved that it is injective. On the next homework, you'll show it is surjective. You can assume this result for now. So you also have a bijection $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.
3. You also have theorems 11.2.4 and 12.1 available to you.

Theorem 13.2 (Cantor)**.** *Suppose X is a set. Let $\mathcal{P}(X)$ be the powerset of X.*

Let f be any function with domain X and codomain $\mathcal{P}(X)$. Then f is not surjective.

In particular, $\mathcal{P}(\mathbb{N})$ is not countable.

To show a function $f : X \longrightarrow Y$ is not surjective, you need to show that there is a $y \in Y$ such that whatever $x \in X$ you pick, you have $f(x) \neq y$.

The hint for proving the above theorem is: $\{x \in X : x \notin f(x)\}$.

14 Comments on August 16th

The student proofs on August 15th and August 16th were of a very high standard. I would go as far as saying that the quality of proofs presented in this class so far have been the highest I have seen in such a class. I am very impressed. Keep up the good work!

I might not have time to post thorough comments on the student proofs of August 15th and August 16th. However, I will prove theorem 12.1 in the solutions to the second homework. Below I'll give proofs for theorem 13.1 and 13.2. They will not differ substantially from what we saw in class. But, by posting them, you can spend more time thinking about them.

Proof of theorem 13.1. We wish to show that $\mathbb{Q}$ is countable. By definition of countability, we have to construct a surjection $\mathbb{N} \longrightarrow \mathbb{Q}$. Our idea is to construct such a surjection as the composition of functions which we have already encounted.

Recall from the first homework the functions $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, $j : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Q}$, $k : \mathbb{N} \longrightarrow \mathbb{Z}$ defined by $h(m,n) = 2^{m-1}(2n-1)$, $j(m,n) = \frac{m}{n}$, and

$$k(n) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd;} \\ -\frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

We also have the function $k \times 1_{\mathbb{N}} : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Z} \times \mathbb{N}$ defined by $(k \times 1_{\mathbb{N}})(m,n) = (k(m), n)$.

To help the reader, we draw the functions relevant to our argument in a diagram.

$$\begin{tikzcd} \mathbb{N} & \mathbb{N} \times \mathbb{N} \arrow[l, "h"'] \arrow[r, "k \times 1_{\mathbb{N}}"] & \mathbb{Z} \times \mathbb{N} \arrow[r, "j"] & \mathbb{Q} \end{tikzcd}$$

We proved on the first homework that h is injective. We prove on the second homework that h is surjective. Thus, h is a bijection. Theorem 11.2.4 tells us that h has an inverse $h^{-1} : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$. Moreover, since h^{-1} has h an inverse, theorem 11.2.4 (again!) tells us that h^{-1} is a bijection. In particular, h^{-1} is surjective.

We prove on the second homework that k is a bijection. In particular, k is a surjection. The identity function of a set is always a bijection. Thus, $1_{\mathbb{N}} : \mathbb{N} \longrightarrow \mathbb{N}$ is a bijection. In particular, $1_{\mathbb{N}}$ is a surjection. The next lemma applies to show that $k \times 1_{\mathbb{N}}$ is a surjection too.

Finally, on the second homework we show that j is a surjection.

We need one more key fact: the composition of two surjections is a surjection too. This is part 4 theorem of 12.1. We use this twice. First, it tells us that $j \circ (k \times 1_{\mathbb{N}})$ is a surjection. Second, it tells us that $((j \circ (k \times 1_{\mathbb{N}})) \circ h^{-1}$ is a surjection.

$$\begin{tikzcd} \mathbb{N} \arrow[r, "h^{-1}"] & \mathbb{N} \times \mathbb{N} \arrow[r, "k \times 1_{\mathbb{N}}"] & \mathbb{Z} \times \mathbb{N} \arrow[r, "j"] & \mathbb{Q} \end{tikzcd}$$

This completes the proof that $\mathbb{Q}$ is countable. □

Lemma 14.1. *Suppose that $f : X \longrightarrow X'$ and $g : Y \longrightarrow Y'$ are surjections. Then the function*

$$f \times g : X \times Y \longrightarrow X' \times Y'$$

defined by $(f \times g)(x,y) = (f(x), g(y))$ is a surjection.

Remark 14.2. In the lemma above, I swapped things a little from what I wrote in lecture.

Proof of lemma. Suppose that $f : X \longrightarrow X'$ and $g : Y \longrightarrow Y'$ are surjections. Define $f \times g$ as in the theorem statement. We wish to show that $f \times g$ is a surjection. So let $(x', y') \in X' \times Y'$.

Since f is a surjection, we can choose an $x \in X$ such that $f(x) = x'$.

Since g is a surjection, we can choose a $y \in Y$ such that $g(y) = y'$.

Notice that $(f \times g)(x, y) = (f(x), g(y)) = (x', y')$.

Thus, $f \times g$ is surjective. □

Proof of theorem 13.2. Suppose X is a set. Let $\mathcal{P}(X)$ be the powerset of X.

Let f be any function with domain X and codomain $\mathcal{P}(X)$.

We wish to show that f is not surjective.

First, let's understand f a little better. Suppose that $x \in X$. Then $f(x) \in \mathcal{P}(X)$. By definition of the powerset, this means $f(x) \subseteq X$. Because of this unusual setup, it is reasonable to ask the question "is $x \in f(x)$?" Moreover, asking this question for every $x \in X$, we can define a set

$$C := \{x \in X : \ x \notin f(x)\}.$$

(I've used the letter C in honor of Cantor.) We have $C \subseteq X$. By definition of powerset, this means $C \in \mathcal{P}(X)$.

Let's now turn to our task. Suppose for contradiction that f is surjective. Then we can find an $x \in X$ such that $f(x) = C$. There are two cases:

1. $x \in C$.

   By definition of C, this gives $x \notin f(x)$. Because $f(x) = C$, this is the same as saying $x \notin C$. This contradicts the case that we're working in.

2. $x \notin C$.

   By definition of C, this gives $x \in f(x)$. Because $f(x) = C$, this is the same as saying $x \in C$. This contradicts the case that we're working in.

Both cases lead to a contradiction, so our assumption that f is surjective must be false. □

Remark 14.3. I was surprised that both students used a proof by contradiction. It turned out I was pleasantly surprised because I think this might the proof easier to read. However, it is possible to make the argument without "proof by contradiction."

Alternative proof of theorem 13.2. Suppose X is a set. Let $\mathcal{P}(X)$ be the powerset of X. Let f be any function with domain X and codomain $\mathcal{P}(X)$. We wish to show that f is not surjective. Define $C := \{x \in X : \ x \notin f(x)\}$. We will show that for any $x \in X$, $f(x) \neq C$.

Let $x \in X$. There are two cases:

1. $x \in C$.

   By definition of C, this gives $x \notin f(x)$.

   We conclude $C \nsubseteq f(x)$ because C contains x and $f(x)$ does not contain x. Thus, $f(x) \neq C$.

2. $x \notin C$.

   By definition of C, this gives $x \in f(x)$.

   We conclude $f(x) \nsubseteq C$ because $f(x)$ contains x and C does not contain x. Thus, $f(x) \neq C$.

In both cases, we conclude that $f(x) \neq C$. Since x was an arbitrary element of X, we have shown $f(x) \neq C$ for all $x \in X$. Thus, f is not surjective because it never obtains the value C. □

Remark 14.4. Some people find the argument that the real numbers are uncountable easier.

Theorem 14.5. *Let $[0,1)$ be the set $\{y \in \mathbb{R} : 0 \leq y < 1\}$.*

Let f be any function with domain $\mathbb{N}$ and codomain $[0,1)$. Then f is not surjective.

Proof. Let $[0,1)$ be as in the theorem statement, and let f be any function with domain $\mathbb{N}$ and codomain $[0,1)$. We wish to show that f is not surjective.

First, let's think about f a little. f provides us with a list of real numbers between 0 and 1.
$f(1)$ can be expressed in decimals as $0 \cdot a_{1,1}\ a_{1,2}\ a_{1,3}\ a_{1,4}\ a_{1,5}\ a_{1,6}\ a_{1,7}\ a_{1,8}\ \cdots$
$f(2)$ can be expressed in decimals as $0 \cdot a_{2,1}\ a_{2,2}\ a_{2,3}\ a_{2,4}\ a_{2,5}\ a_{2,6}\ a_{2,7}\ a_{2,8}\ \cdots$
$f(3)$ can be expressed in decimals as $0 \cdot a_{3,1}\ a_{3,2}\ a_{3,3}\ a_{3,4}\ a_{3,5}\ a_{3,6}\ a_{3,7}\ a_{3,8}\ \cdots$
$f(4)$ can be expressed in decimals as $0 \cdot a_{4,1}\ a_{4,2}\ a_{4,3}\ a_{4,4}\ a_{4,5}\ a_{4,6}\ a_{4,7}\ a_{4,8}\ \cdots$
$f(5)$ can be expressed in decimals as $0 \cdot a_{5,1}\ a_{5,2}\ a_{5,3}\ a_{5,4}\ a_{5,5}\ a_{5,6}\ a_{5,7}\ a_{5,8}\ \cdots$
$f(6)$ can be expressed in decimals as $0 \cdot a_{6,1}\ a_{6,2}\ a_{6,3}\ a_{6,4}\ a_{6,5}\ a_{6,6}\ a_{6,7}\ a_{6,8}\ \cdots$
$f(7)$ can be expressed in decimals as $0 \cdot a_{7,1}\ a_{7,2}\ a_{7,3}\ a_{7,4}\ a_{7,5}\ a_{7,6}\ a_{7,7}\ a_{7,8}\ \cdots$
$f(8)$ can be expressed in decimals as $0 \cdot a_{8,1}\ a_{8,2}\ a_{8,3}\ a_{8,4}\ a_{8,5}\ a_{8,6}\ a_{8,7}\ a_{8,8}\ \cdots$
$\cdots$
We will define a number $y \in [0,1)$ which is not on this infinite list.
Let $y = 0 \cdot a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ \cdots$
where

$$a_n = \begin{cases} 8 & \text{if } a_{n,n} \neq 8; \\ 0 & \text{if } a_{n,n} = 8. \end{cases}$$

Suppose $n \in \mathbb{N}$. We cannot have $f(n) = y$ because $f(n)$ and y differ at the n-th decimal place.

Thus, f is not surjective because it never obtains the value y. □

Theorem 14.6. *Let f be any function with domain $\mathbb{N}$ and codomain $\mathbb{R}$. Then f is not surjective.*

Proof. Let f be any function with domain $\mathbb{N}$ and codomain $\mathbb{R}$.

Suppose for contradiction f is surjective. Let $g : \mathbb{R} \longrightarrow [0,1)$ be defined by

$$g(x) = \begin{cases} x & \text{if } x \in [0,1); \\ 0 & \text{if } x \notin [0,1). \end{cases}$$

Then g is surjective, so $g \circ f : \mathbb{N} \longrightarrow [0,1)$ is surjective. This contradicts the previous theorem. □

Finally, you might ask "do $\mathcal{P}(\mathbb{N})$ and $\mathbb{R}$ have the same cardinality?"

Theorem 14.7. *$\mathcal{P}(\mathbb{N})$ and $\mathbb{R}$ have the same cardinality.*

Proof. Define $t : \mathcal{P}(\mathbb{N}) \longrightarrow \mathbb{R}$ by $t(I) = \sum_{i \in I} 3^{-i}$. "$t$" stands for "ternary;" t is injective.
Define $d : \mathbb{R} \longrightarrow \mathcal{P}(\mathbb{Q})$ by $d(r) = \{q \in \mathbb{Q} :\ q < r\}$. "$d$" stands for "Dedekind;" d is injective.
We proved in theorem 13.1 that there exists a surjection $w : \mathbb{N} \longrightarrow \mathbb{Q}$. "$w$" stands for "whoa."
Define $s : \mathbb{Q} \longrightarrow \mathbb{N}$ by $s(q) = \min\{n \in \mathbb{N} :\ w(n) = q\}$. "$s$" stands for "section;" s is injective.
Define $\mathcal{P}(s) : \mathcal{P}(\mathbb{Q}) \longrightarrow \mathcal{P}(\mathbb{N})$ by $\mathcal{P}(s)(X) = \{s(q) :\ q \in X\}$. $\mathcal{P}(s)$ is injective.
$\mathcal{P}(s) \circ d : \mathbb{R} \longrightarrow \mathcal{P}(\mathbb{N})$ is an injection.
In summary, we have two injections $t : \mathcal{P}(\mathbb{N}) \longrightarrow \mathbb{R}$ and $\mathcal{P}(s) \circ d : \mathbb{R} \longrightarrow \mathcal{P}(\mathbb{N})$.
From this data, the Cantor-Bernstein theorem provides a bijection $\mathcal{P}(\mathbb{N}) \longrightarrow \mathbb{R}$.
`http://en.wikipedia.org/wiki/Schroder-Bernstein_theorem` □

15 Homework due on August 20th

1. **Theorem 15.1.** *The function $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $h(m, n) = 2^{m-1}(2n-1)$ is surjective.*

2. (a) Prove that your $j : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Q}$ from last week is surjective.

   (b) Prove that your $k : \mathbb{N} \longrightarrow \mathbb{Z}$ from last week is a bijection by giving an inverse $k' : \mathbb{Z} \longrightarrow \mathbb{N}$ and checking that it is an inverse. You're using theorem 11.2.4.

3. Hand in your proofs for theorem 12.1.

4. Define a function $f : \mathbb{R} \longrightarrow \mathbb{R}$ which is injective, but not surjective.

   An example is the exponential function $\exp : \mathbb{R} \longrightarrow \mathbb{R}$. However, I also want you to be able to prove that your function is injective and not surjective without assuming properties of such complicated functions. I ban you from using transcendental functions like exp, cos, and sin.

5. Let $X = \{x \in \mathbb{R} : \ -1 < x < 1\}$. Define $g : X \longrightarrow \mathbb{R}$ by $g(x) = \frac{x}{1-|x|}$.

   Prove that g is a bijection.

   Remark. In all the questions that follow, we change our convention regarding $\mathbb{N}$.

   $\mathbb{N}$ will mean $\{0, 1, 2, \ldots\}$, *not* $\{1, 2, 3, \ldots\}$.

6. **Theorem 15.2.** *Let*

$$X = \left\{ x : \mathbb{N} \longrightarrow \{0, 1\} : \ \left\{ i \in \mathbb{N} : \ x(i) = 1 \right\} \textit{ is finite} \right\}.$$

   The function $b_\infty : X \longrightarrow \mathbb{N}$ defined by

$$b_\infty(x) = \sum_{i=0}^{\infty} x(i) \cdot 2^i$$

   is well-defined and bijective.

   I expect for you to find this harder.

   My strategy would be to start by trying to prove this directly until you have flashbacks from last week and realize that you already know most of what you need to know.

   In particular, you should be referencing question 4 from the last homework which says that for each $n \in \{1, 2, 3, \ldots\}$, the function

$$b_n : \{0, 1\}^n \longrightarrow \{0, 1, 2, \ldots, 2^n - 1\}, \ (x_0, x_1, \ldots, x_{n-1}) \longmapsto \sum_{i=0}^{n-1} x_i \cdot 2^i$$

   is a bijection.

7. Define a bijection $\left\{ x : \mathbb{N} \longrightarrow \{0, 1\} \right\} \longrightarrow \mathcal{P}(\mathbb{N})$. You only need to prove it to yourself.

8. Is there a bijection

$$\left\{ x : \mathbb{N} \longrightarrow \{0, 1\} : \ \left\{ i \in \mathbb{N} : \ x(i) = 1 \right\} \text{ is finite} \right\} \longrightarrow \left\{ x : \mathbb{N} \longrightarrow \{0, 1\} \right\}?$$

   You can assume Cantor's results to justify your claim.

16 The set up in theorem 15.2

Consider the function $x : \mathbb{N} \longrightarrow \{0, 1\}$ defined by

$$\begin{aligned}
x(0) &= 1\\
x(1) &= 0\\
x(2) &= 0\\
x(3) &= 1\\
x(4) &= 1\\
x(5) &= 0\\
x(6) &= 0\\
x(7) &= 0\\
x(8) &= 1\\
x(9) &= 0\\
x(10) &= 0\\
x(11) &= 0\\
x(12) &= 0\\
x(13) &= 0\\
x(14) &= 0\\
x(15) &= 0\\
x(16) &= 0\\
x(17) &= 0\\
x(18) &= 0\\
x(n) &= 0 \ \text{ if } n > 18.
\end{aligned}$$

For what values of $\mathbb{N}$ does this function return 1? Just 0, 3, 4, and 8. That is,

$$\{i \in \mathbb{N} : \ x(i) = 1\} = \{0, 3, 4, 8\}.$$

This is certainly a finite set. So x meets the conditions to be in X. We have $x \in X$.

What is $b_\infty(x)$? It's

$$\begin{aligned}
&1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 0 \cdot 2^6 + 0 \cdot 2^7 + 1 \cdot 2^8\\
&+ 0 \cdot 2^9 + 0 \cdot 2^{10} + 0 \cdot 2^{11} + 0 \cdot 2^{12} + 0 \cdot 2^{13} + 0 \cdot 2^{14} + 0 \cdot 2^{15} + 0 \cdot 2^{16} + 0 \cdot 2^{17} + 0 \cdot 2^{18} + \dots
\end{aligned}$$

which is $1 + 8 + 16 + 256 = 281$.

We could worry about that "...," but it just consists of

$$0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + \dots$$

so we don't have to worry: it's just 0.

For an arbitrary $x \in X$, a similar thing will happen because $\{i \in \mathbb{N} : \ x(i) = 1\}$ is finite.

17 Solutions to homework 2

1. **Theorem 17.1.** *The function $h : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ defined by $h(m,n) = 2^{m-1}(2n-1)$ is surjective.*

   Proof. We wish to show that $h : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ defined by $h(m,n) = 2^{m-1}(2n-1)$ is surjective. So let $N \in \mathbb{N}\times\mathbb{N}$. We want to find a pair $(m,n) \in \mathbb{N}\times\mathbb{N}$ such that $h(m,n) = N$.

   Let m be the maximum element in the set
   $$\left\{ m \in \mathbb{N} : \frac{N}{2^{m-1}} \in \mathbb{N} \right\}.$$

   Notice that $\frac{N}{2^{m-1}}$ is odd, since otherwise we could divide N by a larger power of 2. This means that $\frac{N}{2^{m-1}} + 1$ is even, and we can divide it by 2 to obtain a natural number: let $n = \frac{N}{2^m} + \frac{1}{2}$. We see that $g(m,n) = 2^{m-1}(2n-1) = 2^{m-1}(2\cdot(\frac{N}{2^m} + \frac{1}{2}) - 1) = N$, which completes the proof that h is surjective. □

2. (a) Define $j : \mathbb{Z}\times\mathbb{N} \longrightarrow \mathbb{Q}$ by $(m,n) \longmapsto \frac{m}{n}$.
   By definition of the rational numbers, every $q \in \mathbb{Q}$ is of the form $\frac{m}{n}$ where $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. So j is surjective.

   (b) Define $k : \mathbb{N} \longrightarrow \mathbb{Z}$ and $r : \mathbb{Z} \longrightarrow \mathbb{N}$ (I changed my mind about naming it k') by
   $$k(n) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd;} \\ -\frac{n}{2} & \text{if } n \text{ is even;} \end{cases} \qquad \text{and} \qquad r(n) = \begin{cases} 2n+1 & \text{if } n \geq 0; \\ -2n & \text{if } n < 0. \end{cases}$$

   We wish to show that $r \circ k = 1_{\mathbb{N}}$ and $k \circ r = 1_{\mathbb{Z}}$.
   Let n be an odd natural number. Then $k(n) = \frac{n-1}{2} \geq 0$. Thus,
   $$(r\circ k)(n) = r(k(n)) = r\left(\frac{n-1}{2}\right) = 2\left(\frac{n-1}{2}\right) + 1 = n = 1_{\mathbb{N}}(n).$$

   Let n be an even natural number. Then $k(n) = -\frac{n}{2} < 0$. Thus,
   $$(r\circ k)(n) = r(k(n)) = r\left(-\frac{n}{2}\right) = -2\left(-\frac{n}{2}\right) = n = 1_{\mathbb{N}}(n).$$

   We have shown $r \circ k = 1_{\mathbb{N}}$.
   Let n be an integer with $n \geq 0$. Then $r(n) = 2n+1$ is an odd natural number. Thus,
   $$(k\circ r)(n) = k(r(n)) = k(2n+1) = \frac{(2n+1)-1}{2} = n = 1_{\mathbb{Z}}(n).$$

   Let n be an integer with $n < 0$. Then $r(n) = -2n$ is an even natural number. Thus,
   $$(k\circ r)(n) = k(r(n)) = k(-2n) = -\frac{(-2n)}{2} = n = 1_{\mathbb{Z}}(n).$$

   We have shown $k \circ r = 1_{\mathbb{Z}}$.
   Since we have shown k has an inverse theorem 11.2.4 tells us that k is a bijection.

3. Suppose X, Y, and Z are sets, and $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ are functions.

   (a) Suppose $g \circ f$ is injective. We want to show f is injective.
   So let $x_1, x_2 \in X$ and suppose $f(x_1) = f(x_2)$. We want to show that $x_1 = x_2$.
   Applying g gives $g(f(x_1)) = g(f(x_2))$.
   By definition of the composite $g \circ f$, this is the same as $(g \circ f)(x_1) = (g \circ f)(x_2)$.
   Since $g \circ f$ is injective, this gives $x_1 = x_2$. Thus, f is injective.

   (b) Suppose $g \circ f$ is surjective. We want to show g is surjective.
   So let $z \in Z$. We want to find a $y \in Y$ such that $g(y) = z$.
   Since $g \circ f$ is surjective, we can choose an $x \in X$ such that $(g \circ f)(x) = z$.
   Let $y = f(x)$. We just have to show that $g(y) = z$. We have

   $$g(y) = g(f(x)) = (g \circ f)(x) = z.$$

   The first equality is because $y = f(x)$. The second uses the definition of $g \circ f$. And the third follows from how we chose x.
   This completes the proof that g is surjective.

   (c) Suppose f and g are injective. We want to show $g \circ f$ is injective.
   So let $x_1, x_2 \in X$ and suppose $(g \circ f)(x_1) = (g \circ f)(x_2)$. We want to show $x_1 = x_2$.
   By definition of $g \circ f$, this is the same as $g(f(x_1)) = g(f(x_2))$.
   Since g is injective, this gives $f(x_1) = f(x_2)$.
   Since f is injective, this gives $x_1 = x_2$.
   Thus, $g \circ f$ is injective.

   (d) Suppose f and g are surjective. We want to show $g \circ f$ is surjective.
   So let $z \in Z$. We wish to find an $x \in X$ such that $(g \circ f)(x) = z$.
   Since g is surjective, we can choose a $y \in Y$ such that $g(y) = z$.
   Since f is surjective, we can choose an $x \in X$ such that $f(x) = y$.
   We have $(g \circ f)(x) = g(f(x)) = g(y) = z$. Thus, $g \circ f$ is surjective.

4. Define $f : \mathbb{R} \longrightarrow \mathbb{R}$ by

   $$f(x) = \begin{cases} x-1 & \text{if } x < 0; \\ 0 & \text{if } x = 0; \\ x+1 & \text{if } x > 0; \end{cases}$$

   f is injective, but not surjective, and this is fairly easy to prove.

   Another example is $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \frac{x}{1+|x|}$. The fact that this function is injective but not surjective follows from the next exercise.

5. Let $X = \{x \in \mathbb{R} : \ -1 < x < 1\}$.

   Define $g : X \longrightarrow \mathbb{R}$ by $g(x) = \frac{x}{1-|x|}$.

   Define $f : \mathbb{R} \longrightarrow X$ by $f(x) = \frac{x}{1+|x|}$.

   We will show that $g \circ f = 1_{\mathbb{R}}$ and that $f \circ g = 1_X$.

   Let $x \in \mathbb{R}$. Then

$$(g \circ f)(x) = g(f(x)) = g\left(\frac{x}{1+|x|}\right) = \frac{\frac{x}{1+|x|}}{1 - \left|\frac{x}{1+|x|}\right|} = \frac{\frac{x}{1+|x|}}{1 - \frac{|x|}{1+|x|}} = \frac{\frac{x}{1+|x|}}{\frac{1}{1+|x|}} = x = 1_{\mathbb{R}}(x).$$

   Let $x \in X$. Then

$$(f \circ g)(x) = f(g(x)) = f\left(\frac{x}{1-|x|}\right) = \frac{\frac{x}{1-|x|}}{1 + \left|\frac{x}{1-|x|}\right|} = \frac{\frac{x}{1-|x|}}{1 + \frac{|x|}{1-|x|}} = \frac{\frac{x}{1-|x|}}{\frac{1}{1-|x|}} = x = 1_X(x).$$

   Thus, g has an inverse and theorem 11.2.4 tells us that g is a bijection.

   Moreover, f is a bijection. If we enlarge the codomain of f to be all of $\mathbb{R}$, we lose surjectivity and preserve injectivity, providing the second example that we gave in 4.

6. Let X and b_∞ be as in the theorem statement.

   The formula for $b_\infty(x)$ makes sense because the condition on a function $x : \mathbb{N} \longrightarrow \{0, 1\}$ being in X ensures that we never have to add infinitely many non-zero terms.

   To show b_∞ is injective, let $x_1, x_2 \in X$ and suppose that $b_\infty(x_1) = b_\infty(x_2)$. We wish to show that $x_1 = x_2$. Let

$$N_1 = \max\{i \in \mathbb{N} : \ x_1(i) = 1\}, \ N_2 = \max\{i \in \mathbb{N} : \ x_2(i) = 1\}, \text{ and } N = \max\{N_1, N_2\}.$$

   Then

$$x_1(i) = x_2(i) = 0 \text{ for } i > N. \tag{17.2}$$

   Recall that question 4 from the last homework says that for each $n \in \{1, 2, 3, \ldots\}$, the function

$$b_n : \{0, 1\}^n \longrightarrow \{0, 1, 2, \ldots, 2^n - 1\}, \ (x_0, x_1, \ldots, x_{n-1}) \longmapsto \sum_{i=0}^{n-1} x_i \cdot 2^i$$

   is a bijection. Because of (17.2), we have

$$\begin{aligned} b_{N+1}(x_1(0), x_1(1), x_1(2), \ldots, x_1(N)) &= b_\infty(x_1) \\ &= b_\infty(x_2) = b_{N+1}(x_2(0), x_2(1), x_2(2), \ldots, x_2(N)). \end{aligned}$$

   Since b_{N+1} is injective, we obtain

$$(x_1(0), x_1(1), x_1(2), \ldots, x_1(N)) = (x_2(0), x_2(1), x_2(2), \ldots, x_2(N)).$$

   Together with (17.2), this shows that $x_1 = x_2$. So b_∞ is injective.

   To show b_∞ is surjective, let $N \in \mathbb{N}$. We wish to find an $x \in X$ with $b_\infty(x) = N$. We have $N \in \{0, 1, 2, \ldots, 2^{N+1} - 1\}$, and since b_{N+1} is surjective, we can find $(x_0, x_1, \ldots, x_N)$ such that $b_{N+1}(x_0, x_1, \ldots, x_N) = N$. Define $x : \mathbb{N} \longrightarrow \{0, 1\}$ by $x(i) = x_i$ if $i \leq N$ and $x(i) = 0$ if $i > N$. Then $b_\infty(x) = b_{N+1}(x_0, x_1, \ldots, x_N) = N$. Thus, b_∞ is surjective.

7. We have a bijection $\mathrm{Fib}_1 : \Big\{x : \mathbb{N} \longrightarrow \{0,1\}\Big\} \longrightarrow \mathcal{P}(\mathbb{N})$, defined by $x \longmapsto \Big\{i \in \mathbb{N} :\ x(i) = 1\Big\}$.
8. Suppose for contradiction that there is a bijection (W stands for "wannabe")

$$W : \left\{x : \mathbb{N} \longrightarrow \{0,1\} :\ \Big\{i \in \mathbb{N} :\ x(i) = 1\Big\} \text{ is finite}\right\} \longrightarrow \left\{x : \mathbb{N} \longrightarrow \{0,1\}\right\}.$$

   Then $\mathrm{Fib}_1 \circ W \circ b_\infty^{-1} : \mathbb{N} \longrightarrow \mathcal{P}(\mathbb{N})$ is a bijection. This contradicts Cantor's result that $\mathcal{P}(\mathbb{N})$ is uncountable. Thus, there cannot exist such a bijection W.

18 The reason for the last three questions of homework 2

I was trying to lead you to thinking about the following...

Define $\mathrm{Fib}_1 : \Big\{x : \mathbb{N} \longrightarrow \{0,1\}\Big\} \longrightarrow \mathcal{P}(\mathbb{N})$ by $x \longmapsto \Big\{i \in \mathbb{N} :\ x(i) = 1\Big\}$ and define X to be

$$\left\{x : \mathbb{N} \longrightarrow \{0,1\} :\ \mathrm{Fib}_1(x) \text{ is finite}\right\}.$$

We can draw the following diagram of sets and functions.

$$\begin{tikzcd}
 & \Big\{x : \mathbb{N} \longrightarrow \{0,1\}\Big\} \arrow[r, "\mathrm{Fib}_1", "\cong"'] & \mathcal{P}(\mathbb{N}) \\
\mathbb{N} & X \arrow[l, "b_\infty", "\cong"'] \arrow[u, "\text{include}"] \arrow[r, "\overline{\mathrm{Fib}_1}", "\cong"'] & \{A \subset \mathbb{N} :\ A \text{ is finite}\} \arrow[u, "\text{include}"']
\end{tikzcd}$$

Along the bottom are some sets with same cardinality as $\mathbb{N}$. Along the top are some sets with the same cardinality as $\mathcal{P}(\mathbb{N})$. This shows that the jump in cardinality occurs as a result of looking at *all* subsets of $\mathbb{N}$ instead of just the *finite* ones.

19 Lecture on August 20th and 21st: Equivalence relations

Definition 19.1. Suppose X is a set. A *relation* on a set X is a subset of $X \times X$. If $\mathcal{R} \subseteq X \times X$ is a relation, we write $(x_1, x_2) \in \mathcal{R}$ and $x_1 \mathcal{R} x_2$ interchangeably.

Example 19.2.

1. The "equals" relation on a set X is the set
$$\Delta = \{(x, x) : \ x \in X\}.$$
2. The "not equals" relation on a set X is the set
$$\{(x_1, x_2) \in X \times X : \ x_1 \neq x_2\} = (X \times X) \setminus \Delta$$
3. The *universal relation* on a set X is the whole of $X \times X$.

Example 19.3.

1. The non-strict order relation on the set of real numbers is the set
$$\{(x_1, x_2) \in \mathbb{R} \times \mathbb{R} : \ x_1 \leq x_2\}.$$
2. The strict order relation on the set of real numbers is the set
$$\{(x_1, x_2) \in \mathbb{R} \times \mathbb{R} : \ x_1 < x_2\}.$$
3. The "distance is less than 1" relation on the real numbers is the set
$$\{(x_1, x_2) \in \mathbb{R} \times \mathbb{R} : |x_1 - x_2| < 1\}.$$

Example 19.4.

1. For a set X, the subset relation on $\mathcal{P}(X)$ is the relation
$$\{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) : \ A \subseteq B\}.$$
2. For a set X, the "these subsets overlap relation" is the relation
$$\{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) : \ A \cap B \neq \emptyset\}.$$

Definition 19.5. A relation $\mathcal{R}$ on a set X is said to be:

- *reflexive* **iff** for all $x \in X$, $x \mathcal{R} x$;
- *symmetric* **iff** for all $x_1, x_2 \in X$, if $x_1 \mathcal{R} x_2$, then $x_2 \mathcal{R} x_1$;
- *transitive* **iff** for all $x_1, x_2, x_3 \in X$, if $x_1 \mathcal{R} x_2$ and $x_2 \mathcal{R} x_3$, then $x_1 \mathcal{R} x_3$.

Example 19.6.

1. The "equals" relation on a set X is reflexive, symmetric, and transitive.
2. The "not equals" relation on a set X with two or more elements is not reflexive, symmetric, and not transitive.
3. The *universal relation* on a set X is reflexive, symmetric, and transitive.
4. The non-strict order relation on $\mathbb{R}$ is reflexive, not symmetric, and transitive.
5. The strict order relation on $\mathbb{R}$ is not reflexive, not symmetric, and transitive.
6. The "distance is less than 1" relation on $\mathbb{R}$ is reflexive, symmetric, and not transitive.
7. For a nonempty set X, the subset relation on $\mathcal{P}(X)$ is reflexive, not symmetric, and transitive.
8. For a set X with more than four elements, the "these subsets overlap relation" is not reflexive (since $\emptyset$ is not related to itself), symmetric, and not transitive.

Example 19.7. Suppose $X = \{0, 1\}$. Then $X \times X$ has 4 elements, so $\mathcal{P}(X \times X)$ has 2^4 elements. There are 16 relations on X:

	0	1
0	●	●
1	●	●

	0	1
0	●	●
1		●

	0	1
0	●	
1	●	●

	0	1
0	●	
1		●

	0	1
0	●	●
1	●	

	0	1
0	●	●
1		

	0	1
0	●	
1	●	

	0	1
0	●	
1		

	0	1
0		●
1	●	●

	0	1
0		●
1		●

	0	1
0		
1	●	●

	0	1
0		
1		●

	0	1
0		●
1	●	

	0	1
0		●
1		

	0	1
0		
1	●	

	0	1
0		
1		

The relations described in the first row are reflexive. The rest are not reflexive.

The relations described in the first and last column are symmetric. The rest are not symmetric.

We found out in class that you find transitivity far more confusing.

The statement "if $x_1 \mathcal{R} x_2$ and $x_2 \mathcal{R} x_3$, then $x_1 \mathcal{R} x_3$" does not say very much if $x_1 = x_2$ or $x_2 = x_3$. If $x_1 \neq x_2$ and $x_2 \neq x_3$, then it becomes either "if $0\mathcal{R}1$ and $1\mathcal{R}0$, then $0\mathcal{R}0$," or "if $1\mathcal{R}0$ and $0\mathcal{R}1$, then $1\mathcal{R}1$." So if $0\mathcal{R}1$, $1\mathcal{R}0$, and $\mathcal{R}$ is not reflexive, then $\mathcal{R}$ is not transitive. So the relations in the first column which are not in the first row are not transitive. The other relations are transitive.

Definition 19.8. A relation $\mathcal{R}$ on a set X is said to be an *equivalence relation* **iff** $\mathcal{R}$ is reflexive, symmetric and transitive. Symbols like $\sim$, $\approx$, $\equiv$, are often used to denote a relation that is known to be an equivalence relation.

Example 19.9. Fix $n \in \mathbb{N}$. We can define a relation on $\mathbb{Z}$ by declaring $a \sim_n b$ **iff**

$$\text{there exists a } d \in \mathbb{Z} \text{ such that } a - b = dn.$$

$\sim_n$ is an equivalence relation. It is left as a homework exercise for you to check this.

Example 19.10. Define a relation on $\mathbb{Z} \times \mathbb{N}$ by declaring $(m_1, n_1) \sim_{\mathbb{Q}} (m_2, n_2)$ **iff** $m_1 n_2 = m_2 n_1$.

This is an equivalence relation.

I'll leave it to you to show that $\sim_{\mathbb{Q}}$ is reflexive and symmetric. Here is my proof that $\sim_{\mathbb{Q}}$ is transitive...

Suppose $(m_1, n_1), (m_2, n_2), (m_3, n_3) \in \mathbb{Z} \times \mathbb{N}$, $(m_1, n_1) \sim_{\mathbb{Q}} (m_2, n_2)$, and $(m_2, n_2) \sim_{\mathbb{Q}} (m_3, n_3)$.

We wish to show that $(m_1, n_1) \sim_{\mathbb{Q}} (m_3, n_3)$, that is, that $m_1 n_3 = m_3 n_1$.

Note:

- Since $(m_1, n_1) \sim_{\mathbb{Q}} (m_2, n_2)$, we have $m_1 n_2 = m_2 n_1$.
- Since $(m_2, n_2) \sim_{\mathbb{Q}} (m_3, n_3)$, we have $m_2 n_3 = m_3 n_2$.

There are now two cases.

1. $m_2 = 0$.

   First, we use the first bullet point to see

   $$m_1 n_2 = m_2 n_1 = 0 \cdot n_1 = 0.$$

   Since $n_2 \in \mathbb{N}$, $n_2 \neq 0$, so we must have $m_1 = 0$.

   Next, we use the second bullet point to see

   $$m_3 n_2 = m_2 n_3 = 0 \cdot n_3 = 0.$$

   Again, since $n_2 \neq 0$, we must have $m_3 = 0$.

   We conclude that $m_1 n_3 = 0 \cdot n_3 = 0 = 0 \cdot n_1 = m_3 n_1$.

2. $m_2 \neq 0$.

   Using the first and second bullet points together gives

   $$(m_1 n_2)(m_2 n_3) = (m_2 n_1)(m_3 n_2).$$

   Factoring out $(m_2 n_2)$ from both sides gives

   $$(m_2 n_2)(m_1 n_3) = (m_2 n_2)(m_3 n_1). \tag{19.11}$$

   We are in the case that $m_2 \neq 0$. Since $n_2 \in \mathbb{N}$, $n_2 \neq 0$ and $m_2 n_2 \neq 0$.

   The function $\mathbb{Z} \to \mathbb{Z}$, $i \longmapsto (m_2 n_2) i$ is injective. Thus, equation (19.11) gives $m_1 n_3 = m_3 n_1$.

Definition 19.12.

1. Let $\sim$ be an equivalence relation on a set X and let $x \in X$. The set
$$[x] := \{x' \in X : \; x \sim x'\}$$
is called the *equivalence class of* x.

2. The element in the brackets [ ] in the above notation is called a *representative* for the equivalence class.

Definition 19.13. Let $\sim$ be an equivalence relation on a set X. The *set of equivalence classes* of $\sim$ is the set
$$X/{\sim} := \{[x] : \; x \in X\}.$$

Example 19.14. Consider the relation $\sim_5$ on $\mathbb{Z}$. Write $[a]_5$ for the equivalence class of a. Then
$$\begin{aligned}[0]_5 &= \{0, 5, 10, 15, 20, 25, \ldots\} \cup \{-5, -10, -15, -20, -25, \ldots\} = [5]_5 \\ [2]_5 &= \{2, 7, 12, 17, 22, 27, \ldots\} \cup \{-3, -8, -13, -18, -23, -28 \ldots\} = [-13]_5\end{aligned}$$

We usually wite $\mathbb{Z}/5$ for $\mathbb{Z}/{\sim_5}$ and say "$\mathbb{Z}$ mod 5." We have
$$\mathbb{Z}/5 = \Big\{[a]_5 : \; a \in \mathbb{Z}\Big\} = \Big\{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\Big\}.$$

Example 19.15. Let's write Q (not $\mathbb{Q}$) for the set of equivalence classes
$$(\mathbb{Z} \times \mathbb{N})/{\sim_{\mathbb{Q}}} = \Big\{[(m,n)]_{\mathbb{Q}} : \; (m,n) \in \mathbb{Z} \times \mathbb{N}\Big\}.$$

This set is attempting to be the rationals $\mathbb{Q}$. It does an excellent job, but before we call it $\mathbb{Q}$, we should give it an addition and multiplication.

Theorem 19.16. *Let Q be the set of equivalence classes $(\mathbb{Z} \times \mathbb{N})/{\sim_{\mathbb{Q}}}$.*

Define addition $+ : Q \times Q \longrightarrow Q$ and multiplication $\cdot : Q \times Q \longrightarrow Q$ by
$$\begin{aligned}[(m_1, n_1)]_{\mathbb{Q}} + [(m_2, n_2)]_{\mathbb{Q}} &:= [(m_1 n_2 + m_2 n_1, n_1 n_2)]_{\mathbb{Q}} \\ [(m_1, n_1)]_{\mathbb{Q}} \cdot [(m_2, n_2)]_{\mathbb{Q}} &:= [(m_1 m_2, n_1 n_2)]_{\mathbb{Q}}.\end{aligned}$$

These operations are well-defined.

Remark 19.17. What does well-defined mean?

Suppose we do $[(2,3)]_{\mathbb{Q}} + [(1,4)]_{\mathbb{Q}}$. Our definition gives $[(2 \cdot 4 + 1 \cdot 3, 3 \cdot 4)]_{\mathbb{Q}}$ which is $[(11,12)]_{\mathbb{Q}}$.

However, $[(2,3)]_{\mathbb{Q}} = [(4,6)]_{\mathbb{Q}}$ because $(2,3) \sim_{\mathbb{Q}} (4,6)$ because $2 \cdot 6 = 4 \cdot 3$.

Also, $[(1,4)]_{\mathbb{Q}} = [(3,12)]_{\mathbb{Q}}$ because $(1,4) \sim_{\mathbb{Q}} (3,12)$ because $1 \cdot 12 = 3 \cdot 4$.

Using our definition to do $[(4,6)]_{\mathbb{Q}} + [(3,12)]_{\mathbb{Q}}$ gives $[(4 \cdot 12 + 3 \cdot 6, 6 \cdot 12)]_{\mathbb{Q}}$ which is $[(66,72)]_{\mathbb{Q}}$.

We did not change our inputs to the addition, but we did change the "name" of our inputs. Our definition of addition explicitly depends on the name we use. For this reason, our answers $[(11,12)]_{\mathbb{Q}}$, $[(66,72)]_{\mathbb{Q}}$ look different. Thankfully $[(11,12)]_{\mathbb{Q}} = [(66,72)]_{\mathbb{Q}}$ because $11 \cdot 72 = 66 \cdot 12$.

Proving the theorem requires checking that this always works out. That is, that changing names does not make things go silly.

20 Student proofs on August 21st

Theorem 20.1. *Let $\sim$ be an equivalence relation on a set X and $x_1, x_2 \in X$.*

The following are equivalent:

1. $x_1 \sim x_2$.

2. $[x_1] = [x_2]$.

3. $[x_1] \cap [x_2] \neq \emptyset$.

Proof. Let $\sim$ be an equivalence relation on a set X and $x_1, x_2 \in X$.

- 1. $\implies$ 2.

  Suppose $x_1 \sim x_2$. We must show that $[x_1] = [x_2]$.

  Let $x' \in [x_2]$. By definition of $[x_2]$, we have $x_2 \sim x'$. Since $x_1 \sim x_2$ and $x_2 \sim x'$, transitivity gives $x_1 \sim x'$, which shows $x' \in [x_1]$. Thus, $[x_2] \subseteq [x_1]$.

  Since $x_1 \sim x_2$, symmetry gives $x_2 \sim x_1$. Repeating the argument just given with the roles of x_1 and x_2 swapped shows $[x_1] \subseteq [x_2]$.

  Thus, $[x_1] = [x_2]$.

- 2. $\implies$ 3.

  Suppose $[x_1] = [x_2]$. Since $\sim$ is reflexive, $x_1 \sim x_1$, and this gives $x_1 \in [x_1] = [x_1] \cap [x_2]$.

  Thus, $[x_1] \cap [x_2] \neq \emptyset$.

- 3. $\implies$ 1.

  Suppose $[x_1] \cap [x_2] \neq \emptyset$. Then we can choose an element $x' \in [x_1] \cap [x_2]$.

  Since $x' \in [x_1]$, we have $x_1 \sim x'$.

  Since $x' \in [x_2]$, we have $x_2 \sim x'$. By symmetry, we obtain $x' \sim x_2$.

  Since $x_1 \sim x'$ and $x' \sim x_2$, transitivity gives $x_1 \sim x_2$.

□

21 Student proofs on August 22nd

Prove theorem 19.16.

Remark 21.1. My proof of transitivity in example 19.10 might feel a little weird.

The point of the equivalence relation in that example is to enable a construction of the rationals from the integers. For this reason, in my proof of transitivity, I was careful not to use any properties of rational numbers. I only used properties of integers and natural numbers.

(One such property I used is that for $n \in \mathbb{Z} \setminus \{0\}$, the function $\mathbb{Z} \longrightarrow \mathbb{Z}$, $i \longmapsto ni$ is injective. It is a bit weird to think about how you'd prove this without using division.)

In your proof of theorem 19.16, you should only use (properties of) integers and natural numbers, even if thinking about rational numbers is useful.

Proof of theorem 19.16. Let Q be the set of equivalence classes $(\mathbb{Z} \times \mathbb{N})/{\sim_{\mathbb{Q}}}$.

Define addition $+ : Q \times Q \longrightarrow Q$ and multiplication $\cdot : Q \times Q \longrightarrow Q$ by

$$\begin{aligned}[(m_1, n_1)]_{\mathbb{Q}} + [(m_2, n_2)]_{\mathbb{Q}} &:= [(m_1n_2 + m_2n_1, n_1n_2)]_{\mathbb{Q}}\\ [(m_1, n_1)]_{\mathbb{Q}} \cdot [(m_2, n_2)]_{\mathbb{Q}} &:= [(m_1m_2, n_1n_2)]_{\mathbb{Q}}.\end{aligned}$$

We wish to show whese operations are well-defined. What is the issue here? Let's focus on addition.

Suppose $(m_1, n_1), (m_1', n_1'), (m_2, n_2), (m_2', n_2') \in \mathbb{Z} \times \mathbb{N}$, that

$$[(m_1, n_1)]_{\mathbb{Q}} = [(m_1', n_1')]_{\mathbb{Q}} \text{ and } [(m_2, n_2)]_{\mathbb{Q}} = [(m_2', n_2')]_{\mathbb{Q}}.$$

The definition of addition says that $[(m_1, n_1)]_{\mathbb{Q}} + [(m_2, n_2)]_{\mathbb{Q}}$ is equal to

$$[(m_1n_2 + m_2n_1, n_1n_2)]_{\mathbb{Q}}.$$

The definition of addition also says that $[(m_1', n_1')]_{\mathbb{Q}} + [(m_2', n_2')]_{\mathbb{Q}}$ is equal to

$$[(m_1'n_2' + m_2'n_1', n_1'n_2')]_{\mathbb{Q}}.$$

We need to show that $[(m_1n_2 + m_2n_1, n_1n_2)]_{\mathbb{Q}} = [(m_1'n_2' + m_2'n_1', n_1'n_2')]_{\mathbb{Q}}$. By theorem 20.1, it is enough to show that $(m_1n_2 + m_2n_1, n_1n_2) \sim_{\mathbb{Q}} (m_1'n_2' + m_2'n_1', n_1'n_2')$. By the definition of $\sim_{\mathbb{Q}}$, it is enough to show that

$$(m_1n_2 + m_2n_1) \cdot (n_1'n_2') = (m_1'n_2' + m_2'n_1') \cdot (n_1n_2). \tag{21.2}$$

We assummed $[(m_1, n_1)]_{\mathbb{Q}} = [(m_1', n_1')]_{\mathbb{Q}}$ and $[(m_2, n_2)]_{\mathbb{Q}} = [(m_2', n_2')]_{\mathbb{Q}}$. By theorem 20.1, these give $(m_1, n_1) \sim_{\mathbb{Q}} (m_1', n_1')$ and $(m_2, n_2) \sim_{\mathbb{Q}} (m_2', n_2')$. By definition of $\sim_{\mathbb{Q}}$, these give

$$m_1n_1' = m_1'n_1 \text{ and } m_2n_2' = m_2'n_2. \tag{21.3}$$

Reiterating, we know (21.3) and want to show (21.2). Here goes:

$$\begin{aligned}(m_1n_2 + m_2n_1) \cdot (n_1'n_2') &= (m_1n_2) \cdot (n_1'n_2') + (m_2n_1) \cdot (n_1'n_2')\\ &= (m_1n_1') \cdot (n_2n_2') + (m_2n_2') \cdot (n_1n_1')\\ &= (m_1'n_1) \cdot (n_2n_2') + (m_2'n_2) \cdot (n_1n_1')\\ &= (m_1'n_2') \cdot (n_1n_2) + (m_2'n_1') \cdot (n_1n_2) = (m_1'n_2' + m_2'n_1') \cdot (n_1n_2).\end{aligned}$$

The first and last equalities are expanding and factoring, respectively.

The second and fourth equalities come from swapping the order of some multiplications.

The third equality follows directly from (21.3).

We have checked (21.2), and this completes checking that addition is well-defined.

Checking that multiplication is well-defined is similar, but less messy. □

22 Lecture on August 22st

Theorem 22.1. *Suppose X and Y are sets and that $f : X \longrightarrow Y$ is a function.*

Suppose, in addition, that we have an equivalence relation $\sim$ on X, and that for all $x_1, x_2 \in X$, if $x_1 \sim x_2$, then $f(x_1) = f(x_2)$.

Then f induces a well-defined function

$$\overline{f} : X/\!\sim \longrightarrow Y,\ [x] \longmapsto f(x).$$

Proof. Suppose X and Y are sets and that $f : X \longrightarrow Y$ is a function.

Suppose, in addition, that we have an equivalence relation $\sim$ on X, and that for all $x_1, x_2 \in X$, if $x_1 \sim x_2$, then $f(x_1) = f(x_2)$. We wish to show that

$$\overline{f} : X/\!\sim \longrightarrow Y,\ [x] \longmapsto f(x)$$

is well-defined.

What is our worry? What if $[x_1] = [x_2]$, but our formula for $\overline{f}$ leads to $\overline{f}([x_1]) \neq \overline{f}([x_2])$? We just need to give the reason that this does not happen.

Suppose that $[x_1] = [x_2]$. By theorem 20.1, we have $x_1 \sim x_2$. We assumed that if $x_1 \sim x_2$, then $f(x_1) = f(x_2)$, and so we can conclude that $f(x_1) = f(x_2)$. Thus,

$$\overline{f}([x_1]) = f(x_1) = f(x_2) = \overline{f}([x_2]).$$

□

Theorem 22.2. *Suppose X and Y are sets and that $f : X \longrightarrow Y$ is a function.*

*Define a relation on X by declaring $x_1 \sim x_2$ **iff** $f(x_1) = f(x_2)$.*

Then $\sim$ is an equivalence relation. Moreover, f induces an injection

$$\overline{f} : X/\!\sim \longrightarrow Y,\ [x] \longmapsto f(x).$$

Example 22.3. Consider the surjective function from the homework

$$j : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Q},\ (m, n) \longmapsto \frac{m}{n}$$

and the equivalence relation $\sim_{\mathbb{Q}}$.

We have $(m_1, n_1) \sim_{\mathbb{Q}} (m_2, n_2)$ if and only if $j(m_1, n_1) = j(m_2, n_2)$.

Thus, j induces a well-defined function

$$\overline{j} : (\mathbb{Z} \times \mathbb{N})/\!\sim_{\mathbb{Q}} \longrightarrow \mathbb{Q},\ [(m, n)]_{\mathbb{Q}} \longmapsto \frac{m}{n}.$$

As in the proof of the theorem, you can show $\overline{j}$ is injective.

One sees that $\overline{j}$ is surjective too. Thus, $\overline{j}$ is a bijection.

23 Homework due on August 27th

1. (a) Find relations R_1, R_2, R_3 on $X = \{0, 1, 2\}$ such that:

   i. R_1 is reflexive, not symmetric, and not transitive.

   ii. R_2 is not reflexive, symmetric, and transitive.

   iii. R_3 is not reflexive, not symmetric, and not transitive.

   (b) Can you give examples of relations on $X = \{0, 1, 2\}$ which give
   the remaining five combinations of (not) reflexive, (not) symmetric, (not) transitive?

2. Prove that $\sim_{\mathbb{Q}}$ is reflexive and symmetric.

3. Fix $n \in \mathbb{N}$. Prove that $\sim_n$ is an equivalence relation.

4. **Theorem 23.1.** *Fix $n \in \mathbb{N}$, and let $\mathbb{Z}/n$ be the set of equivalence classes $\mathbb{Z}/\sim_n$.*
   Define addition $+ : \mathbb{Z}/n \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/n$ and multiplication $\cdot : \mathbb{Z}/n \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/n$ by

   $$[a]_n + [b]_n := [a + b]_n$$
   $$[a]_n \cdot [b]_n := [ab]_n.$$

   These operations are well-defined.

5. Let $n \in \mathbb{N}$.

   Write n using the decimal system: $n = \sum_{i=0}^{\infty} a_i \cdot 10^i$, and for all i, $a_i \in \{0, 1, 2, \ldots, 9\}$.

   Making use of $\sim_9$, prove that n is divisible by 9 if and only if the sum of its digits $\sum_{i=0}^{\infty} a_i$ is divisible by 9.

6. Prove theorem 22.2.

24 Solutions to previous homework

1. (a) i. $R_1 = \{(1,1),\ (2,2),\ (3,3),\ (1,2),\ (2,3)\}$.
   ii. $R_2 = \emptyset$.
   iii. $R_3 = \{(1,2),\ (2,3)\}$.

   (b) Equals, not equals, non-strict order relation, strict order relation, distance less than 1.

2. Let $(m,n) \in \mathbb{Z}\times\mathbb{N}$. The trivial equation $mn = mn$ shows, by definition of $\sim_{\mathbb{Q}}$, that $(m,n) \sim_{\mathbb{Q}} (m,n)$. Thus, $\sim_{\mathbb{Q}}$ is reflexive.

   Let $(m_1,n_1),(m_2,n_2) \in \mathbb{Z}\times\mathbb{N}$, and suppose $(m_1,n_1) \sim_{\mathbb{Q}} (m_2,n_2)$. By definition of $\sim_{\mathbb{Q}}$, we have $m_1n_2 = m_2n_1$. Thus, $m_2n_1 = m_1n_2$, which shows that $(m_2,n_2) \sim_{\mathbb{Q}} (m_1,n_1)$, so $\sim_{\mathbb{Q}}$ is symmetric.

3. (a) Let $a \in \mathbb{Z}$. We want to show $a \sim_n a$.
   Let $d = 0$. Then $d \in \mathbb{Z}$ and $a - a = 0 = dn$. Thus, $a \sim_n a$.
   So $\sim_n$ is reflexive.

   (b) Let $a,b \in \mathbb{Z}$. Suppose that $a \sim_n b$. We want show that $b \sim_n a$.
   Since $a \sim_n b$, we can pick a $d' \in \mathbb{Z}$ such that $a - b = d'n$. Let $d = -d'$, so $d \in \mathbb{Z}$.
   Then $b - a = -(a-b) = -d'n = (-d')n = dn$. Thus, $b \sim_n a$.
   So $\sim_n$ is symmetric.

   (c) Let $a,b,c \in \mathbb{Z}$. Suppose that $a \sim_n b$ and $b \sim_n c$. We want show that $a \sim_n c$.
   Since $a \sim_n b$, we can pick a $d_1 \in \mathbb{Z}$ such that $a - b = d_1n$.
   Since $b \sim_n c$, we can pick a $d_2 \in \mathbb{Z}$ such that $b - c = d_2n$.
   Let $d = d_1 + d_2$, so $d \in \mathbb{Z}$.
   Then $a - c = (a-b) + (b-c) = d_1n + d_2n = (d_1+d_2)n = dn$. Thus, $a \sim_n c$.
   So $\sim_n$ is transitive.

4. I'll just do multiplication (since that is harder).

   Suppose $a, a', b, b' \in \mathbb{Z}$, $[a]_n = [a']_n$, and $[b]_n = [b']_n$.

   By theorem 20.1, we have $a \sim_n a'$ and $b \sim_n b'$.

   By definition of $\sim_n$, we can find $d_1, d_2 \in \mathbb{Z}$ such that $a - a' = d_1n$ and $b - b' = d_2n$.

   Let $d = (d_1b + a'd_2)$.

   Then $ab - a'b' = (a-a')b + a'(b-b') = (d_1n)b + a'(d_2n) = (d_1b + a'd_2)n = dn$.

   So $ab \sim_{\mathbb{Q}} a'b'$. By theorem 20.1, we have $[ab]_{\mathbb{Q}} = [a'b']_{\mathbb{Q}}$.

   This shows multipication is well-defined.

5. Let $n \in \mathbb{N}$.

   Write n using the decimal system: $n = \sum_{i=0}^{\infty} a_i \cdot 10^i$, and for all i, $a_i \in \{0, 1, 2, \ldots, 9\}$.

   Although the sum goes to infinity, only finitely many of the terms are non-zero, so it is really a finite sum.

   First, using the addition and multiplication in the previous question we see that

$$[n]_9 = \left[\sum_{i=0}^{\infty} a_i \cdot 10^i\right]_9 = \sum_{i=0}^{\infty} [a_i \cdot 10^i]_9 = \sum_{i=0}^{\infty} [a_i]_9 \cdot [10^i]_9 = \sum_{i=0}^{\infty} [a_i]_9 \cdot [10]_9^i.$$

   Because $10 - 1 = 9 \cdot 1$, $10 \sim_9 1$, and so $[10]_9 = [1]_9$.

   Thus, we see that $[n]_9$ is equal to

$$\sum_{i=0}^{\infty} [a_i]_9 \cdot [1]_9^i = \sum_{i=0}^{\infty} [a_i]_9 \cdot [1^i]_9 = \sum_{i=0}^{\infty} [a_i]_9 \cdot [1]_9 = \sum_{i=0}^{\infty} [a_i \cdot 1]_9 = \sum_{i=0}^{\infty} [a_i]_9 = \left[\sum_{i=0}^{\infty} a_i\right]_9 .$$

   By definition of $\sim_9$, we see that n is divisible by 9 if and only if $[n]_9 = [0]_9$.

   We also see that the sum of n's digits is divisible by 9 if and only if $\left[\sum_{i=0}^{\infty} a_i\right]_9 = [0]_9$.

   The calculation made above shows that $[n]_9 = \left[\sum_{i=0}^{\infty} a_i\right]_9$.

   Thus, n is divisible by 9 if and only if the sum of n's digits is divisible by 9.

6. Hmm. Maybe later.

25 Midterm

1. Let X and Y be sets.

   Here's a fun fact: if X and Y are finite sets, X has n elements, and Y has m elements, then $X \times Y$ has nm elements.

   Write down sets A and B in terms of X and Y so that:

   - your definitions of A and B make sense regardless of what X and Y are;
   - if X and Y are finite sets, X has n elements, and Y has m elements, then A has $n+m$ elements, and B has n^m elements.

   Solution: $A = (\{0\} \times X) \cup (\{1\} \times Y)$.

   $B = \{f \subseteq Y \times X : \ f$ is a function with domain Y and codomain $X\}$.

2. (a) Suppose that X, Y, and Z are sets.
   Suppose that $f_1 : X \longrightarrow Y$, $f_2 : X \longrightarrow Y$ are functions.
   Suppose that $g : Y \longrightarrow Z$ is an *injective* function.
   Prove that if $g \circ f_1 = g \circ f_2$, then $f_1 = f_2$.

   Solution: Suppose $g \circ f_1 = g \circ f_2$.
   We want to show that $f_1 = f_2$. So let $x \in X$. We wish to show that $f_1(x) = f_2(x)$.
   Since $g \circ f_1 = g \circ f_2$, we have $(g \circ f_1)(x) = (g \circ f_2)(x)$. By definition of composition of functions, this is the same as $g(f_1(x)) = g(f(x_2))$.
   Since g is injective, this gives $f_1(x) = f_2(x)$.
   Since $x \in X$ was arbitrary, this shows that $f_1 = f_2$.

   (b) Suppose that X, Y, and Z are sets.
   Suppose that $f : X \longrightarrow Y$ is a *surjective* function.
   Suppose that $g_1 : Y \longrightarrow Z$, $g_2 : Y \longrightarrow Z$ are functions.
   Prove that if $g_1 \circ f = g_2 \circ f$, then $g_1 = g_2$.

   Solution: Suppose $g_1 \circ f = g_1 \circ f$.
   We want to show that $g_1 = g_2$. So let $y \in Y$. We wish to show that $g_1(y) = g_2(y)$.
   Since f is surjective, we can choose an $x \in X$ such that $f(x) = y$.
   Then $g_1(y) = g_1(f(x)) = (g_1 \circ f)(x) = (g_2 \circ f)(x) = g_2(f(x)) = g_2(y)$.
   Here, we have used $f(x) = y$ in the first and last equality.
   The second and fourth equalities use the definition of the composition of functions.
   The middle equality uses the assumption that $g_1 \circ f = g_2 \circ f$.
   Since $y \in Y$ was arbitrary, this shows that $g_1 = g_2$.

3. (a) Let X and Y be sets.
Say what it means for a function $f : X \longrightarrow Y$ to be a *bijection*.

Solution: f is a bijection **iff** f is injective and surjective.

(b) Define a bijection $\pi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Z}$.

Solution: Define $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ by $h(m, n) = 2^{m-1}(2n - 1)$, and $k : \mathbb{N} \longrightarrow \mathbb{Z}$ by

$$k(n) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd;} \\ -\frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

Let $\pi = k \circ h$.

4. (a) Define the concept of a *relation* $\mathcal{R}$ *on a set* X.

Solution: A relation on a set X is a subset $\mathcal{R}$ of the Cartesian product $X \times X$.

(b) Let X be a set and recall the definition of a function in terms of its graph.
This means that a function $f : X \longrightarrow X$ can be viewed as a relation on X.
Which functions $X \longrightarrow X$, when viewed as relations, are equivalence relations?

Solution: Suppose $f \subseteq X \times X$ is a function which, when viewed as a relation, is reflexive.
Given $x \in X$, we have $(x, x) \in f$ which means $f(x) = x$.
Thus, the only reflexive function is the identity $1_X : X \longrightarrow X$.
This is the “equality” equivalence relation.

(c) Let $\sim$ be the relation on $\mathbb{N} \times \mathbb{N}$ defined by declaring

$$(m_1, n_1) \sim (m_2, n_2) \ \textbf{ iff } \ m_1 + n_2 = m_2 + n_1.$$

$\sim$ is an equivalence relation. Write $(\mathbb{N} \times \mathbb{N})/\sim$ for the set of equivalence classes.
Define a bijection $g : (\mathbb{N} \times \mathbb{N})/\sim \longrightarrow \mathbb{Z}$.
You should should check that your function is well-defined, but need not prove it’s a bijection.

Solution: Define $g : (\mathbb{N} \times \mathbb{N})/\sim \longrightarrow \mathbb{Z}$ by $g([(m, n)]) = m - n$.
We’ll show g is well-defined.
Suppose that $(m_1, n_1) \sim (m_2, n_2)$. By definition of $\sim$, we have $m_1 + n_2 = m_2 + n_1$.
Thus, $g([(m_1, n_1)]) = m_1 - n_1 = m_2 - n_2 = g([(m_2, n_2)])$, so g is well-defined.

5. Let $\sim$ be the relation on $\mathcal{P}(\mathbb{N})$ defined by declaring

$$A \sim B \ \textbf{iff} \ \text{there exists a bijection } f : A \longrightarrow B.$$

(a) Prove that $\sim$ is symmetric.

Solution: Suppose $A, B \in \mathcal{P}(\mathbb{N})$ and that $A \sim B$.
We wish to show that $B \sim A$.
By definition of $B \sim A$, we have to show that there exists a bijection $g : B \longrightarrow A$.
By definition of $A \sim B$, we know that we can choose a bijection $f : A \longrightarrow B$.
Theorem 11.2.4 tells us that $f : A \longrightarrow B$ has an inverse function $g : B \longrightarrow A$. Since f is an inverse function for g, theorem 11.2.4 also tells us that $g : B \longrightarrow A$ is a bijection.

(b) $\sim$ is an equivalence relation. You may assume this from now on.
Describe the equivalence class $[\{1\}]$ explicitly.

Solution: $\Big\{\{n\} : \ n \in \mathbb{N}\Big\}$.

(c) Let $\mathcal{P}(\mathbb{N})/\!\sim$ be the set of equivalence classes.
Describe $\mathcal{P}(\mathbb{N})/\!\sim$ and say whether $\mathcal{P}(\mathbb{N})/\!\sim$ is finite, countable, or uncountable.

Solution: We claim that

$$\mathcal{P}(\mathbb{N})/\!\sim \ = \ \Big\{[\emptyset]\Big\} \cup \Big\{\big[\{1, 2, \ldots, n\}\big] : \ n \in \mathbb{N}\Big\} \cup \Big\{[\mathbb{N}]\Big\}$$

and that $q : \mathbb{N} \longrightarrow \mathcal{P}(\mathbb{N})/\!\sim$ defined by

$$q(n) = \begin{cases} [\mathbb{N}] & \text{if } n = 1; \\ [\emptyset] & \text{if } n = 2; \\ \big[\{1, 2, \ldots, n-2\}\big] & \text{if } n > 2; \end{cases}$$

is a bijection, so that $\mathcal{P}(\mathbb{N})/\!\sim$ is countably infinite.

26 Comments regarding the midterm and the end of part 1

Acknowledgments on my part:

1. The union part of question 1 was too difficult.
2. 4(b) was too weird.
3. 5(c) was supposed to be a tester.

Criticisms of your exams...

1. Many people could not complete 3(a) correctly.

   This question asked for you to define a *bijection*.

   In the first two weeks of this class, the main content was injective and surjective functions, and proving that various functions are bijections, i.e. both injective and surjective.

   Yet many people did not manage to say that a bijection is an injective and surjective function.

   Some who did manage this decided to give the incorrect definition of injective and/or surjective.

   Definition 6.9 consists of less than 100 symbols.

   You had three weeks to know those symbols, in the correct order, and to practice with them.

2. Many people could not complete 4(a) correctly.

   I know relations might be more confusing. I had at least one student come to office hours very confused about them. However, they spoke with me for 2 hours about the relations examples we did in class, and surprise, surprise, they answered this question correctly.

3. Many people could not complete 3(b) correctly.

   Homework 1, 4(a) asked you to show $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ defined by $h(m, n) = 2^{m-1}(2n - 1)$ is injective. Homework 2, 1 asked you to show it is surjective. Both solutions were posted long before the midterm. We did one of the proofs in class.

   Homework 1, 6(b) asked you for a bijection $k : \mathbb{N} \longrightarrow \mathbb{Z}$. Homework 2, 2(b) asked you to prove it is a bijection. Both solutions were posted long before the midterm.

   In our proof of theorem 13.1 which we covered in class, and which I typed up for you, we used compositions of functions to great effect.

4. The aforementioned questions provided 8 free points.

   At least 6 people scored below 8 points.

5. Question 2 was not well done, and I felt it was the most formulaic on the exam.

   These questions are very similar to ones on the homework and ones that we proved in class.

   To those of you who asked for extra preparation, I advised you to look in any resource for similar results to the ones we had already proved. These are what you would have found. They are very standard results.

   I think Kevin has sent you comments about your homework.

   And so he has surely pointed out when you have done this type of question incorrectly.

   But yet, we still have people giving/using the wrong definition of injection and surjection.

Rant over. What we were doing was clearly not working. Someone once said that "insanity is doing the same thing over and over again and expecting different results" so I'd guess we'd better change something.

See part 2...

This was my original emotional response. Perhaps nerves got the better of some students, and I overreacted. However, I'm still pleased we tried part 2 in a different format!