[SQUEAKING] [RUSTLING] [CLICKING]

**CASEY RODRIGUEZ:** So last time we spoke about-- we covered sets and induction. This time, I want to ask a question about sets, which turns out is actually quite a deep question. I mean, I didn't come up with it myself. This question is at least 150 years old probably.

So the question that I want to ask is if A and B are sets-- or let's phrase it this way, at least a little more efficiently. When do two sets, A and B, have the same size? Now, this is especially interesting if these two sets are not finite, meaning there's not five of them, there's not eight of them, but there's infinitely many members, whatever that means. And I'll actually define what that means.

For example, do the natural numbers and the integers have the same size? Do the natural numbers and the rational numbers have the same size? What about the rational numbers and the real numbers? Even though we haven't defined that yet, you can still keep in mind your notion of the real numbers from calculus.

And so this question is-- why is it deep? Because it depends on this word here, "size," and what exactly that means. So I'm not-- so kind of an answer, this is due to George Cantor. He said that two sets-- so not an answer, but a way of defining size or a way of saying the two sets have the same size. He said two sets have the same size when the two sets-- the elements of the two sets can be paired off, meaning-- and I will make this much more precise in a minute or so.

What does he mean? Or what do I mean? For example, the set a, b, and c and the set 1, 2, and 3. So this one, this set, consists of three letters-- a, b, and c. This set consists of three integers-- 1, 2, and 3. They have the same size because I can essentially pair them off. So a and 1 go together, b and 2 go together, and c and 3 go together, meaning each member of this set gets paired off with an element of this set. And every element of this set gets paired off with a unique element from this set.

Now, to make-- and so this goes under the name of the theory of cardinality or cardinal numbers, if you like. But we won't go too deeply into it. So the way you make-- or the way one makes this pairing off business more precise is using the language of functions.

And you've been dealing with functions since you've been doing calculus. So I'm just going to quickly reintroduce or review some terminology that goes along with functions that will be the precise meaning of this pairing off business that I'm writing here. But just with an eye towards the future, this is why I'm reviewing some of this terminology related to functions.

So a brief review of some terminology for functions-- so let me just recall that if A and B are sets, then function f A B-- so a function's usually written as f colon A arrow to B, meaning it takes elements from A into elements from B. This is a mapping that-- or if you like, an assignment. It assigns to each x in A a unique element which we denote f of x in B.

So one single input, x, gives me a single output. And the input does not give me three outputs. Now, this is what one would call a naive definition probably, not necessarily completely unambiguous. But for us, it suffices.

In the textbook, you can look up a function is unambiguously defined or as a subset of the Cartesian product of A and B, which you would recognize as essentially describing the graph of the function. But then you never use that definition of again. And you essentially use this definition when you think about functions and when you prove properties of function. So this we will just take as our definition. And it will be unambiguous enough for us.

So let f be a function from A to B. If C is a subset of A, we define a set-- so this is f of capital C. So C is not an element of A. It's a subset of A.

And this is a subset of B. This is-- let me write it slightly differently here. This is a set of all y in B such that there exists an x in C such that y equals to f of x. And I could write this a little more efficiently as this is the set of all elements f of x as x ranges over the elements of this subset C.

And if D is a subset of B, we define the set f inverse of D. This is the set of guys that get mapped into D. So I should say this is the inverse image of D, not the inverse of this function f. So the inverse, whatever that means for now, does not necessarily always exist. So this inverse image of the set D always exists. This is the set of all elements in A such that f of x is in D.

So for example, let me-- so 1, 2, 3, 4 and a, b, c, d. And let's suppose 1 goes to a, 2 goes to a, 3 goes to c, 4 goes to d. Then f of the set 1, 2, this is where-- what is the set that gets-- so this is the subset of-- so this you should think of as B, a, b, and c, and D. And then 1, 2, and 3, this is A.

So f of the set of 1, 2-- so 1 gets mapped to a. 2 gets mapped to a. So this is just the set 2. f of the set-- let's go with 1 and 3. 1 gets mapped to a. So this should be a. 1 gets mapped to a. And 3 gets mapped gets mapped to c.

And so a couple of inverse images-- if I look at the inverse image of a, this is equal to the set of all guys that map to a. This is, well, 1 maps to a and 2 maps to a. So this is 1, 2. Now, if I look at the inverse image of a, c, d, what elements get mapped to a, c, and d? Well, 1 and 2 get mapped to a. 3 gets map to c. 4 gets mapped to d. So everything maps into a, C, and d. So this is just the original set or the set A-- 1, 2, 3, 4.

All right, so there's more terminology. And this is what we will mean by when two sets can be paired off. Or this makes that more precise. Let f be a function from A to B. We say that f is injective, or I'll write one-to-one. It should be read one-to-one if f satisfies the following property. f of x1 equals f of x2 implies x1 equals x2.

So injective, or one-to-one, means if I take two different inputs, I get two different outputs. That's essentially what this means. I mean, taking the equivalent-- so equivalently, from a logical standpoint, this statement implying this statement is equivalent to the negation of this statement implying the negation of this statement. So equivalently, this means x not equal to x2 implies f of x1 not equal to f of x2.

So maybe this is clear. If I were to define f as injective if it satisfies this property, maybe that would have been clearer that f takes two different elements to two different elements. But this condition here is typically easier to verify, or at least simpler to state and verify.

So f is surjective or onto if the image of A is B. So let me write that statement out a little bit more. Everything in the set B gets mapped to by something from A. So equivalently, this says that for all y in B there exists an x in A so that f of x equals y.

f is bijective if f is one-to-one and onto. So f is bijective if it's both injective and surjective. So for example, this map that we just drew over here that sends 1 to a, 2 to b-- I mean 2 to a, 3 to c, 4, to d, this is neither injective nor surjective. It's not injective because it takes two different elements to the image in B, namely a. So it takes 1 and 2 to a. It's not surjective because nothing gets mapped to the element b here.

So we've seen that's not surjective. Of course, this map, if I take-- again, imagine this is 1, 2, 3 a, b, c, d. This map here, this function here that takes 1 to a, 2 to b, 3, to c, this is actually injective but not surjective. And then of course, we could change this slightly. And 1 goes to a, 2 goes to b, and 3 goes to b. Then this is surjective but not injective.

Now, the map that sends-- let's switch sides here-- a, b, and c, 1, 2, 3-- a to 1, b to 2, c to 3, this is a bijection, bijective. So if I say something's an injection or surjection or bijection, that just means it's a map that is injective, or, surjective or bijective respectively.

And now, a definition-- so this is really-- there's not much to this definition, but just defining a couple of related functions that are related to a given function. If f goes from A to B, g goes from B to C, the composition g of f is the function which goes from A to C is defined by g of f of x equals g of f of x. And 2, if f is bijective-- so this is the composition of two functions. I didn't write the word composition, but g of f means the composition, or is referred to as a composition.

If f is bijective, then we define the inverse function to f, B to A, by the following. If y is in B, then f inverse of y in A is the unique elements in A such that if I take this element, stick it into f, I get back y. So the inverse of a function only exists for bijective functions, or at least is only defined for bijective functions.

Keep that in mind. Don't confuse that with the inverse image of sets. Although, those two notations look the same. You have an inverse f to the minus 1. f to the minus 1, if it's a function, that is the inverse function. However, if I'm taking f to the minus 1 of a set, that means the inverse image of that set as defined over there.

So bijections, meaning bijective functions, will be what we mean when we say two sets can be paired off. It's what we mean when we-- or at least what Cantor's answer to that original question was, when did two sets have the same size. So this is the notion of cardinality that I alluded to.

So we say two sets, A and B, have the same cardinality if there exists a bijection or a bijective function f from A to B. And so let me just make some notation here. so this is not really new objects I'm defining or operations. This is just some notation.

So when two sets have the same cardinality, we write-- so this is just a shorthand way of writing that two functions have the same cardinality. You should not necessarily think this means taking the absolute value of a set. That doesn't mean anything, all right? This is just shorthand notation for saying two sets have the same cardinality.

If A has the same cardinality as the set 1, 2, 3 up to n, we write A equals n. That's just shorthand for saying that a set has the same cardinality as the natural numbers up to n. So if there exists an injective function-- or I will often say either function or map. You should take those as synonymous.

There exists an injective function f-- if there exists an injective function f from A to B, we write this thing. Again, do not read this as taking the absolute value of some set and that absolute value is less than or equal to the absolute value of the other set because that's meaningless. We haven't said what that means even. This is just shorthand notation.

And if there exists an injection from A to B but they don't have the same cardinality, we write this. So even though this notation of these absolute value things being on the outside of the set makes you think absolute value or should be interpreted as absolute value, it's OK to think as a certain ordering being there, as A having smaller size than B.

We write this because there being an injection from one set to the other means I can pair off elements of A with some elements of B. Maybe I don't get all of the elements of B. But I can pair off some of the elements of A with some of the elements of B. For example, that first map we wrote up there, that says that the set 1, 2, 3 in size is less than or equal to the size of a, b, c, d because we found an injection, an injective map from the first set to the second set.

This third map would say that the size of the set a, b,c is equal to 3, written here, or shorthand written here. And in fact, that first map that we wrote up there, again, is-- so from first map, this says that the set of 1, 2, 3-- in our shorthand notation, absolute value is less than the size of a, b, c, d. So don't think of these as saying the absolute value. It's best to maybe think of this as saying the size of.

All right, so if there exists an injective map or function from one set to another, then the size of A is less than or equal to the size of B. If the size of A is less than or equal to the size of B but the size of A and B are not the same, we write the size of A is less than the size of B. So best to think of those-- this absolute value looking thing as being shorthand for saying the words size of.

Now, I'm not going to prove this. It goes a little bit beyond the scope of this class. But let me just say that this ordering, this inequality, these symbols that we're writing does bear some sort of semblance to the ordering of real numbers in that if I have two real numbers, one is less than or equal to the other and vice versa. So A is less than or equal to B and B is less than or equal to A, then A must equal B.

That is, in fact, true also for this elementary notion of size of sets. And this is-- I mean, it shouldn't surprise you for finite sets necessarily. If I have a pairing of A, if A is no bigger than n and n is no bigger than the size of A, then a should have n elements. But it takes a little bit more to prove for sets which are not finite. So I forgot to write this down. We also say that if the size of A is equal to the size of this finite set 1 through n, we say A is finite.

So this theorem that I'm stating here is the Cantor Schroeder Bernstein theorem, which states that if the size of A is less than or equal to the size of B and the size of B is less than or equal to the size of A, then the size of A equals the size of B. So again, if you're thinking of these in the context of real numbers, one being less than or equal to the other and vice versa, of course, that implies that those two real numbers are equal to each other.

But we're not talking about real numbers. Again, this is just shorthand notation for saying there exists a bijective map from A to B. This means there exists a bijective map from A to the set. This means there exists an injective map from A into this, from a to this set. So this is not a statement about real numbers. This is a statement about cardinality, all right?

OK. So finite sets are sets that you can count if you had n fingers. Now, we would like to be able to define what it means to be able to count a set. So what do I mean by count a set? Meaning, if I had infinite time, I could go through the set counting them-- 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 and so on. I don't need to go anymore.

But what does that process of counting mean? That means, for each element of the set that I'm trying to count, I can pair it off with a natural number-- 1, 2, 3, and so on. So this is how we define countable sets. So if A has the same size as the natural numbers, meaning there exists a bijection from A to the natural numbers, then we say A is countably infinite.

If A is finite, or countably-- I also use a lot of shorthand, but it's not clever shorthand. So you should just be able to sound what-- if you just sound that out, you'll get what word I mean, countably, countably infinite. We say A is countable. So countably infinite means I need all the natural numbers to be able to count off the elements of the set A. Countable means maybe I stop after some point and I've counted all them. So A is finite or it's countably infinite. Otherwise, if a set is not countable, we say it's uncountable.

OK, so let's take a look at a couple of countable sets that maybe don't come off as being countable. The set of-- actually, that's a homework problem. The set of even integers is countable. The set of odd-- so I said integers a minute ago. Maybe I should just say natural numbers. The set of odd natural numbers is countable.

So in fact-- so this is just an aside. So these are two disjoint subsets that make up the natural numbers, even and odd natural numbers. And they both have the same size as the set that they make up. So it's almost like saying the cardinality of the natural numbers is twice the cardinality of the natural numbers, since you would think that the size of N should be the size of this set plus the size of this set, since they are disjoint and they make up the set.

But that's not how cardinality works. You don't just add cardinalities to get the cardinalities. So this is a subtle, interesting thing about cardinalities So Richard Feynman, who won the Nobel Prize in the '60s for his work on QED, described this as saying there are twice as many numbers as numbers.

OK, so let's prove this. So what does this mean? This means we have to be able to find a bijective function from this set to this set or from this set to this set, one or the other. And so in fact, maybe I should-- well, I'll say something about that in a minute.

Well, let me pause. Let me pause this just for a minute. And let me make a few comments about cardinality, which maybe I should have. So this you can think of as a little theorem.

If I have two sets, A has the same size as B, then B has the same size as A. So remember, I mean, what I just said in English is not exactly what those symbols mean. Remember, this means there exists a bijection from A to B This means there exists a bijection from B to A.

So what is the proof of this statement? So let's start off with the hypothesis. Suppose then there exists a bijective map, bijective function f from A to B. Now, if I have a bijection from A to B, then what would be a bijection going from B to A? That would just be the inverse. So this is not the inverse image of sets, like we described, but the actual inverse, which we defined over there. Is a bijection. So B has the same size as A.

One other statement-- so if A and B have the same size and B and C have the same size-- so again, A, B, and C are sets. I should have written that at the beginning. But from this context, you should understand that A, B, and C are sets-- then A and C have the same size. So let's do a proof of that. So let's start with the hypothesis, meaning A has the same size as B and B has the same size as C.

So what did these two statements mean in terms of the definition? That means there exists a bijection from A to B and a bijection from B to C. And this statement-- so let me finish this. And then I'll say what I was going to say. Then there exists bijections f from A to B and g from B to C.

So perhaps I should have said a few more words about why this is true. But I'm going to leave this as an exercise just to pause the lecture and do it yourself. And what I'll write shortly-- for this case, I'll actually prove that the thing I'm going to define is bijection. That should help you.

So let me draw over here off to the side. We have, again, 1, 2, 3, a, b, c. So think of this as f. This is my set A. This is my set B. And then I have alpha, beta, gamma. And a gets mapped to alpha, b, gets mapped to beta, c gets mapped to gamma. So what would be the map going from A down to the set C? Well, perhaps the composition.

1 gets mapped to a, which gets mapped to alpha. So 1 gets mapped to alpha. 2 gets mapped to beta. 3 gets mapped to gamma. How do I build this function out of the things that I know, namely this f and g? Well, this function going from A to C is just the composition of these two functions. So this is off to the side. This is not a part of the proof.

Let h go from A to C be the function g of f of x. So I claim that this function is a bijection. So we want to prove that it's one-to-one and onto, all right? So let's do one-to-one first.

So we this is the part where I'm going to put this in parentheses, meaning what we're doing now. So we're going to prove that h is one-to-one. So that means we have to verify the definition that I've erased. So remember the definition. So let's write it all out.

We first show h is one-to-one. And what this means, according to the definition that I'm now writing over, if h of x1 equals h of x2, then x1 equals x2. So this is what we want to prove. This is the definition of h being one-to-one. So let's start.

If h of x1 equals h of x2, then, in terms of how we've defined h, which is g of f of x, so the composition, then this means g of f of x1 equals g of f of x2. That's just what h is. Now, this statement here-- now g we know is a bijection. We know g is one-to-one. And since g of something equals g of something else and g is one-to-one, this implies that f of x1 equals f of x2. This is since g is one-to-one.

So starting with this and the definition of h being the composition, we conclude that f of x1 has to equal f of x2 because g is one-to-one. Now, since f is also one-to-one-- we are assuming that f and g are bijections. Since f is one-to-one, this implies x1 equals x2, since f is one-to-one. And this is what we wanted to prove. We wanted to start with assuming h of x1 equals h of x2 and prove x1 equals x2, which is what we've done. So thus, we've proven that h is one-to-one. Now, we have to show that it's surjective, that it's onto.

h of A equals C. And again, I'll write out what this means. This means for all y in C-- all right, let me call it [? z-- ?] there exists an x in A such that h of x equals z. Now, we used the fact that f and g were injective to conclude that the composition is injective. So it stands to reason that we're going to use the fact that they're both surjective to prove that h is surjective.

So we need to prove that for all z in C there exists an x in A as such that h of x equals z. So let z be in C. Now, we need to find some x in A that gets mapped to z. We'll use that g and f are both surjective. And what's the picture that goes along with this?

Here's the sets C, B, and A. We have some element of z And we know that since g is surjective, there's some element in B that gets mapped to z by G. But now, since f going from A to B is surjective, there exists some x which maps to y. And then that's the whole argument. That's it. I drew this picture. But now, I just need to turn it into English using the properties and assumptions that I have.

Since g is surjective, there exist a y in B such that g of y equals z. Since f is surjective, there exists an x in A so that f of x equals y. But then if I look at h of x, this is equal to g of f of x, which is equal to g of y, which is equal to z by how we've defined y. Remember, g of y equals z, how we found y and how we found x. Remember, f of x equals this y. And therefore, this map h is onto. And therefore, h is a bijection, proving this theorem. So that should help you. I'll give you many exercises to prove that the inverse of a bijection is a bijection.

So back to what we were doing to begin with. We want to show the set of even natural numbers has the same size as the natural numbers, has the same cardinality, as the natural numbers and the same for the odd ones. So I'm just going to do the odd ones. Again, this will be a small exercise for you to do to prove number 2, the statement for the odd ones. So I'm going to do the even ones. And you can do the odd ones.

You should, if you plan on studying more math, get used to the instructor, professor, research paper writer, textbook author giving out little exercises to make sure that you're following along and that you can do some minor task at some point during the discussion. So we're going to find-- so we want to show that the natural numbers has the same size as the even natural numbers, which is the same as this statement by that first theorem I wrote up there.

Now, that means we need to find a bijection from the natural numbers to the set of even natural numbers. This should be not too bad. I mean, so again, this is off to the side. This is not part of the proof.

What would be the map going from these guys to these guys? Well, I mean, there's several you could choose. But maybe the simplest is 1 gets mapped to 2, 2 gets mapped to 4, 3 gets mapped to 6, 4 gets mapped to 8, 5 to 10, 6 to 12, and so on, and so on.

Now, what is that map? And now, I'll continue the proof. Let f be the function into the even natural numbers defined by f of n equals 2 times n. And so n is a natural number. So this is just formally writing the function that takes 1 to 2, 2 to 4, 3 to 6, 4, to 8, and so on, and so on.

I claim f is a bijection. So I have to show that f is one-to-one and onto. So we'll first show f is one-to-one. So that means that I have to assume f of n1 equals f of n2 and conclude that n1 equals n2.

So let me actually write out what this means again for you to say that f is one-to-one. Is one to one-- i.e. if f of n1 equals f of n2, then n1 equals n2. But this is easy to verify for this function that we've written down because if f of n1 equals f of n2-- so remember, this is what we want to show, all right?

So to show it, I start with my assumption. And I need to conclude n1 equals n2. So suppose f of n1 equals f of n2, my assumption, my hypothesis. And I need to conclude n1 equals n2. Then this implies, by the definition of f, 2 times n2 equals 2 times n2, which, by algebra of just eliminating the 2's, n1 equals n2, which is the conclusion that I want.

So I've proven the statement that if f of n1 equals f of n2, then n1 equals n2. Therefore, f is one-to-one. So thus, f is one-to-one. So now, we want to show f is onto, surjective. I'll write this out again. i.e. For all elements that n are an even number, there exists an n such that f of n equals m.

Now, let m be an even integer. And so not to confuse us, let me write 2 times k. This is the same set. I'm just using a different dummy variable instead of n in my description of the even natural numbers. And let's do that here as well. Again, this is not changing anything. This is just changing the letter I'm using to describe the set, which is inconsequential. But I don't want you to get the false impression that somehow I'm not doing anything at all.

OK, so suppose I have an even integer, then there exists-- simply by the definition of this set, there exists an n natural number so that m equals 2 times n. Then f of this natural number, which is 2 times n, equals m. And therefore, I get something that maps to m. Therefore, f is onto. Therefore, f is a bijection and the two sets have the same cardinality.

All right, so let's-- where are we at? Where should I write? Let's write here. Maybe I'll leave that up because I don't want to-- now, using this-- and I'll probably put this in the homework-- I mean, one can also show-- I should say using this, but one can also show that the integers have the same size as the natural numbers, which, again, is a little bit surprising since the natural numbers are a strict subset of Z.

So what's the proof? So I'm going to draw a picture, then I'm going to write down the function, and then I'm going to leave it as-- actually, I'm going to put it in the homework for you to verify that this function is one-to-one and onto. So let's say there's as many natural numbers as I want to write and as many integers as I want to write.

OK, so what would be a way of mapping the integers in a one-to-one and onto fashion onto the natural numbers? Well, what we could do-- first off, let's send 0 to 1 just to get 0 out of the way. And from then on, now we just need to find a way to map the positive integers and the negative integers onto the natural numbers bigger than 2. And in some way, mentally, we should feel like we can do this because we kind of did it over there, but not explicitly.

So how about we take 1 to 2, 2 to 4, 3 to 6? 4 would then go to 8. And we'll take 1 to 3, minus 2 to 5. I'm getting crossed. And then minus 3 would get sent to 7. So you see that the positive integers get mapped to the even natural numbers and the negative integers get mapped to the odd natural numbers bigger than 1. So I'm not even going to write the proof. This will be part of the homework.

Now, it is a bit surprising that there are twice as many numbers as numbers, not too surprising since these subsets, if you picture them as I've been doing as subsets of the real line, you know they're kind of discrete. So you should be able to count them. What is not-- what is more surprising are-- is whether or not can count subsets that, in some sense, are not discrete. For example, what about the rational numbers?

So this is a theorem that-- and let me just look at those positive rational numbers. In fact, I could take all rational numbers. But for the statement of this theorem, if I look at those rational numbers which are positive, then this has the same size as the natural numbers. You can count the positive rational numbers, which is just a bit crazy to me because here, at least for let's say the integers, once I'm at an integer, I can move to a next biggest one and count that one in some way, right?

And so that makes it believable that I can count the integers. The integers have the same size as the natural numbers, even though that, at first glance, it looks like there's twice as many. But for rational numbers, between any two rational numbers, there's another rational number in between them. You just take the average of those two rational numbers.

So now, this idea of being at a rational number and then moving to the next big one, you can't do that now. So now, it's a little bit up in the air at least whether or not can count the rational numbers. And what I'm saying is that indeed you can. And this will be part of the homework.

I will at least give you an idea of how the proof will go, what we will actually be able to write down, a map based on a simple fact. So let me not write down proof, but let me write down a remark. So we'll actually be able to write down a map based on one simple fact, which is this fundamental theorem of arithmetic, which says that-- so this is just discussion now. More stuff will be written in the homework about this. So just try to follow along.

So the fundamental theorem of arithmetic says that if you have a positive natural number, you can write it in a unique way as a product of prime numbers. Now, for rational numbers, using that, that means you can write every rational number uniquely as a product of prime numbers divided by another product of prime numbers where no two prime numbers-- where the prime numbers up top and the prime numbers at the bottom, none are in common, meaning you've simplified as much as possible.

So instead of 15 over 3-- no, that's not good. Let's say 15 over 30. You have 1/2. So the map that I would take-- so what I'm saying here is that every rational number can be written as some product. So let me not use that notation, but some product p r1 pN rN q1 s1 qn sM where p1, p2, and pN, these are all primes.

q1 up to qN, they're all primes. r1, rN, these are all exponents, positive natural numbers. So rj, sk, these are natural numbers. p1 pN q1 to qM are primes. And for all jk, qj does not equal pk. So there's no prime that appears both up here and down here. We've already simplified that away.

So just so you don't think I'm fooling you, 9/2, which is a positive rational number, this is 3 squared over 2, yeah? I'm not going to do any more. That's it. So the map that we will take from this rational number to a natural number will be this gets mapped to the natural number p1 to r1, pN to rN times now q1 to 2s 1 minus 1 qM 2Sn minus 1.

So basically, I map it to the integer that has this expansion in terms of prime numbers, where now the exponents of these prime numbers is even depending on these exponents on top and the exponents of this one are odd, depending on this exponent on top. So for example, 3 squared over 2, this would get mapped to 3 to the 4 times 2.

So what we'll do in the homework is show that this map is, in fact, a bijection. So those two theorems you will prove in the homework. They won't be too bad. I will leave enough hints. So we've dealt with z. We've dealt with q, essentially.

I mean, so let me actually write down-- this is really a corollary of these two theorems here, which I haven't proved, but you will prove in the homework. So this says that the rationals are countable, all the rationales, not just the positive ones. And what's the proof?

So we know that-- so I'm going to give you a sketch. Should I sketch it or should I write it all out? I'm running a little bit out of time. So maybe I will just tell you why this is true. I mean, all the details are essentially here. I'm just not going to write it as carefully as I've been writing down the proofs before.

So let me write this as the proof sketch. Of course, you can write these-- you can actually use the definitions and write this out. But this is the essential idea. So we have that the size of rational numbers-- so let me-- this has the same size as the rational numbers which are negative. And how do we establish this? Or instead of using the same letter, let's say r, since f of Q equals minus Q is a bijection from the first set to the second set.

If I just take a rational number, positive 1, take its minus, then I get an element of the second set. And this is a bijection. OK, so thus, since this has the same size as the natural numbers, and by that theorem we proved over there, the size of this set is the same as the natural numbers-- so it is countable-- then there exists bijections f going from Q-- so the positive rational numbers-- to the natural numbers and g going from the negative ones to the natural numbers.

So the picture here is-- well, let's not draw the picture yet. OK, so I have these two bijections from the positive rationales to the integers-- this one from the negative rationales to the natural numbers. How do I get a map that goes from all of q now to the natural numbers? Well, let's go in between and go to the integers.

Then I define a function h, which goes now from all of Q to the integers by h of x equals 0 if x equals 0; equals f of x if x is positive; and negative g of x if x is negative. And h is a bijection.

So everything up to this point has been completely fine with the exception of me verifying that this map is a bijection and this map is a bijection. So that's the only parts that I'm leaving out for you to verify. Then h is a bijection. So Q has the same cardinality as integers, which we've shown has the same cardinality as the natural numbers. And therefore, the rationals have the same cardinality as the natural numbers. So they are countably infinite.

So a natural question is-- I mean, is there anything bigger than the natural numbers? Because everything I've written down, this has the size of the natural numbers. We haven't really defined the real numbers well enough yet to make any sort of claim like that about the real numbers. And now, is there just any set that is bigger in size than the natural numbers? The answer to that was unknown. And it's pretty strikingly yes, in fact.

So let me phrase that question. Does there exist a set A such that A has strictly bigger cardinality than the natural numbers, so A is uncountable? So to answer this question astoundingly yes, let me first define for a general object.

If A is a set, we define script p of A. This is the power set of A. This is a set that consists of all subsets of A. So this is a set of all sets B such that B is a subset of A. So for example, if A is the empty set, the power set-- so A is empty. What are the subsets of the empty set?

Well, there's only one subset of the empty set, the empty set. And even though the empty set has no members, its power set has one member. If A equals 1, then the power set of A, the set of all subsets, consists of the empty set and the set itself, 1. And let's do one more. If A is the set 1, 2, then the power set of A, this is the set which consists of the empty set, because this is a subset of this set, the set consisting of 1, because this is a subset of this set, or 2, 1, 2.

Now, notice something. This set had cardinality. Strictly speaking, I should have defined that as having cardinality 0. Yet, its power set has cardinality 1. A has size 1 because it's in one-to-one correspondence with just 1. And its power set has two elements. So it has cardinality 2. I could count them off-- 1, 2.

A has size 2, has two elements. And the power set of A has size 4. It has four different elements-- the empty set, 1, 2, 1, 2. So what one can prove in general and which will appear on the homework is if A has size n-- so it's a finite set of size n, meaning it's in one-to-one correspondence with the numbers 1 up to n-- then its power set is also finite and has cardinality 2 to the n. And you can prove by induction, if you like, that 2 to the n is always bigger than n.

And so a theorem I'll prove next time, which will finish our discussion of sets and cardinality, and then we'll move on to the real numbers, is this theorem due to Cantor, which says that not just for finite sets do we have the power set being, in some sense, strictly bigger than the original set, but for any set. So this theorem due to Cantor is if A is a set, then the cardinality of A is strictly smaller than the cardinality of its power set.

So this definitely answers our question. Does there exist a set with cardinality bigger than the natural numbers? So let me write this as a remark. In fact, maybe I'll state this as another theorem, which just follows immediately from this getting used over and over again, is that the cardinality of the natural numbers, this is less than the cardinality of the power set of the natural numbers, which is less than the cardinality of the power set of the power set of the natural numbers, right? I can now take this as a set and take its power set. And I get a new set with bigger size, which is less than the power set of the power set where-- how many do we have now-- of the power set of natural numbers, and so on.

And formally, this means there's an infinity of infinitudes. There's an infinite number of infinite sizes, one getting strictly-- in some sense, strictly bigger than the previous size. And maybe you're wondering-- there's one more question that's kind of sandwiched in between here, pun intended, is-- let's look at this first guy.

Does there exist a set A such that it has size bigger than natural numbers-- so it's uncountable-- but has size strictly smaller than the power set of the natural numbers. And this question is called the continuum hypothesis, hypothesis because it is independent from one of the standard axiomatic treatments of set theory. But we will not touch this question. This is beyond the scope of this class, but it's an interesting question that's out there that people just don't know.