PROFESSOR: Who can tell me what a proof is? Any ideas of, what is a proof, anyway? Any thoughts? Yeah?

AUDIENCE: It's a chain of statements, each logically supported by the previous ones, that get you from a set of assumptions to a set of conclusions.

PROFESSOR: Very good. I like that. That's very close to what we're going to do here, yeah. Now, that's a special kind of proof, though. That's a mathematical proof. And I'm going to write a definition very close to that in a few minutes.

But proofs exist beyond mathematics. Can anybody think of a higher level notion of what a proof is? That's correct, what you said, but there's a higher meta level notion of what a proof is beyond that. It may have no logical deductions potentially. It may have no assumptions. Any thoughts about a proof?

OK, well, I think generally, a proof is considered, across multiple fields, as a method for ascertaining the truth. And you described one method. Now, by ascertaining, I mean establishing truth, verifying truth. And there's lots of ways to ascertain truth in society, and even within science. What are some examples of ways that we ascertain truth in society? Yeah?

AUDIENCE: Observations, like seeing that piece of chalk will fall to the ground.

PROFESSOR: Observation, experiment and observation-- excellent. And that's the bedrock of physics. I mean, who really knows if there's gravity out there? Well, we observe it. And so we then conclude that's the truth. There's gravity, and we have laws about it.

That's one good way. What's another way of ascertaining truth across scientific disciplines, or beyond science, just in society? How is truth established? What are the ways? Yeah?

AUDIENCE: Well, establishing what's false, you can know what things aren't true. Then that helps you narrow down what is true.

PROFESSOR: Yes, truth-- yeah, that's great. Truth is the opposite of falsehood. How do we establish falsehood? What are the ways in doing that? How you decide something is not true in every day-- yeah?

AUDIENCE: Find counterexamples.

PROFESSOR: Find counterexamples, yeah, that's good. So in fact, even a step more general, sampling. Counterexamples are ways. If you do something, an experiment, ten times, and every time, it comes out one way, that's truth, maybe. But there's fields where that becomes truth. What about other ways?

How are we going to decide if Roger Clemens is guilty of perjury for lying about steroids to Congress? He did it or he didn't. How are we going to decide that? How is that truth going to be ascertained? Yeah?

AUDIENCE: Would it be by examining the evidence that we have?

PROFESSOR: Examining evidence. And who makes the conclusion there?

AUDIENCE: Juries.

PROFESSOR: The jury. Truth is established by juries or judges. You know, Blago-- I can never pronounce his name, the Illinois governor, Blagojevick-- he's guilty. That's the truth of-- not of conspiracy, trying to sell Obama a senate seat, but of lying to the authorities about campaign financing.

OJ is guilty-- not of killing his wife, but of breaking into an apartment to steal back some of his merchandise. So judges and juries make decisions on truth. What are other truths-- bigger truths, even, than judges and juries, in society? There's one really big one that causes a lot of issues. Yeah?

AUDIENCE: Religion.

PROFESSOR: What is it?

AUDIENCE: Religion.

PROFESSOR: Religion, the word of God-- broadly construed here, for religion. Now, that one is really hard to argue about because you believe it. And especially if you're not talking to God regularly and somebody is, well, it's hard to argue about the truth. So you rely on others to interpret it for

you, often-- a priest, or a minister, a rabbi. And it gets complicated, because you can end up with conflicting truths based on who you think you're talking to or who the translator is for you.

Another one is the word of your boss. Whatever the boss says is right. Often in business, the customer is always right. That's the truth, whatever the customer says. With Donald Trump as your boss, you'd better agree or you're fired.

Often in classes, the professor says it, it is true. Because the authority said it. That's not true here. That will not hold.

And one of the nicest things about math that I like a lot is that the youngest student can stand up against the most oldest, most experienced professor, and win an argument on mathematics. I do get pleasure when a student comes up and proves me wrong. I loved it when that student came in, and she showed me what I said really wasn't right when you looked at it carefully or in a different light.

Now, sometimes if I do it on the board here and it's in class, well, that's fun. I feel a little embarrassed afterwards. But it's a good thing about mathematics, is you can have that kind of dialogue.

OK, another one, which is related to the word of God sometimes, is inner conviction-- very popular in computer science, believe it or not, with the mantra, there are no bugs in my program. I can't tell you how many times you hear that.

Closely related is, I don't see why not something is true. And that's a good one, because that transfers the burden of proof to anybody who disagrees with you. You don't have to prove. You just say, I don't see why it's not true. All of a sudden, the other person who's questioning you, it becomes their job to disprove you, which is not so good.

OK, now in mathematics, there's this higher level. And someone stated it very clearly up there. Let me write it up here. In mathematics, we have a mathematical proof is a verification of a proposition by a chain of logical deductions from a set of axioms.

Now, that's a bit of a mouthful. There's three important components here-- propositions, logical deductions, and axioms. And we're going to spend the rest of the class today talking about each of these, and then give an example of a proof. We'll start with propositions.

A proposition is a statement that is either true or false. You may not know which one, but it's

one or the other. A simple example-- 2 plus 3 equals 5. Now, that's a true proposition.

Here's one that's a little more interesting. For all n in the set of natural numbers, n squared plus n plus 41 is a prime number. I know I've used some notation here.

This is-- the upside down A is the for all symbol. How many people have not seen that symbol before? A bunch of you. You're going to see a bunch of symbols here first week.

And that means for every possible choice of n-- and this is in the natural numbers, which is the set 0, 1, 2, 3, and so forth. It's the natural numbers. It's basically the integers, but not negative.

So we're saying for every natural number, i.e. for 0, for 1, for 2, and for 3, and so forth, this expression is a prime. Now, a prime number is a number that is not divisible by any other number besides itself and 1. So 1, 3, 5, 7 are prime. 9 is not because it's 3 times 3.

Now, this part here is called the predicate. And a predicate is a proposition whose truth depends on the value of a variable-- in this case, n. All right, this is referred to as the universe of discourse. It's the space of all the things we're talking about. We're only talking about natural numbers here. This is called a quantifier. We'll see more quantifiers later.

All right, now to see if this proposition is true, we need to make sure that this predicate is true for every natural number n. So let's see if we can check that. Let's try some values.

So we'll try n is 1, 2, 3, and so forth. And we'll compute n squared plus n plus 41. And then we'll check, is it prime? So for n equals 0, n squared plus n plus 41 is 41. Is 41 prime? Yeah, nothing divides 41 but itself and 1.

All right, let's try 1. 1 squared plus 1 plus 41 is 43. Is 43 prime? Yes. Let's try 2. We get 4 plus 2 is 6 plus 41 is 47. Is 47 prime?

AUDIENCE: Yes.

PROFESSOR: Yes. Looking good. 3-- I got 9, 12, 53. Is 53 prime? Yeah. And I could keep on going here. I could go down to 20. I get 420-- 461. In fact, that is a prime. And I could just keep on going here. Go down to 39. I get 1,601. You can check. That is a prime.

The first 40 values of n, the proposition is true. The predicate is true. It is prime. Now, this is a great example because in a lot of fields-- physics, for example; statistics, often-- you checked 40 examples. That's above and beyond the call of duty. It's always true. So yeah, this must be

true, right?

No, wrong. Often, you'll see this in a lot of scientific fields. It is not true. Can anybody give me an example of n for which n squared plus n plus 41 is not prime? Yeah?

AUDIENCE: 40.

PROFESSOR: 40, good. Let's see about 40. 40 squared plus 40 plus 41 is 1,681. What's that equal? 41 squared. So it is not prime. Somebody give me an obvious example where it's not prime.

AUDIENCE: 41.

PROFESSOR: 41-- yeah, 41 squared, we get everything is divided by 41. But 40 is the first break-point. So the first 40 examples work, and then it failed. So this proposition is false, even though it was looking pretty good.

There's a reason I'm doing this. In fact, I'm going to do it some more here. I'm going to beat you over the head with it. Here's a famous in mathematics statement. a to the fourth plus b to the fourth plus c to the fourth equals d to the fourth has no positive integer solutions. That is a proposition.

Now, this proposition was conjectured to be true by Euler in 1769. Euler's a big honcho in math. We still talk about him a lot even though he's been dead for centuries. It was unsolved for over 2 centuries. Mathematicians worked on it.

It was finally disapproved by a very clever fellow named Noam Elkies 218 years later after it was conjectured. He worked at that other school down the street. And he came up with this. a equals 95,800. b equals 217,519. c equals 414,560. You don't have to remember these numbers. We're not going to quiz you on that-- 422,481.

Now, he claims-- I've never personally checked it, but presumably, people have-- you plug those in here, and you have an equality. So he says. So in fact, the correct proposition is there does exist a, b, c, d in the positive natural numbers such that a the fourth plus b to the fourth plus c to the fourth equals d to the fourth.

I used a new quantifier here called there exists. Instead of an upside down A, it's a backwards E. Don't ask me why. That's what it is.

The plus means you can't have 0 or negative numbers. So these are the positive natural

numbers. And here's your predicate, which of course, the truth of this depends on the values of a, b, c and d. It took a long time to figure out that actually, there was a solution here. Obviously, everything they tried until that time failed.

Let me give you another one. 313 x cubed plus y cubed equals z cubed has no positive integer solutions. This turns out to be false. But the shortest, smallest counter-example has over 1,000 digits. This one was easy. It only has six digits. So there's no way ever you'd use a computer to exhaustively search 1,000 digit numbers here to show it's false.

Now, of course, some of you are probably thinking, why on earth would I care if 313 times x cubed plus y cubed equals z cubed has a solution? And that probably won't be the last time that thought occurs to you during the term. And why on earth would anybody ever try to even find a solution to that? I mean, mathematicians are sort of a rare breed.

Now, actually in this case, that's really important in practice. This equation is an example of what's called an elliptic curve-- elliptic curve. You study these if you're really a specialist in mathematics in graduate school, or if you work for certain three-letter agencies because it's central to the understanding of how to factor large integers. That means factoring, showing that-- what was it-- 1,681 is 41 times 41.

And I said, OK, who cares about factoring? Well, factoring is the way to break cryptosystems like RSA, which are used for everything that we do electronically today. You have a Paypal account. You buy something online. You're using SSL. They're all using cryptosystems, almost all of which are based on number theory. And in particular, they're based on factoring. And if you can find good solutions to things like this, or solutions to things like this, all of a sudden, you can get an angle and a wedge on factoring.

And it's because of that that now RSA uses 1,000 digit moduluses instead of hundred digit moduluses like they used to use, because people figured out how to factor and how to break the cryptosystem. If you could break those cryptosystems, well, you can't rule the world, but it's close.

All right, so we'll talk more about this the week after next when we do number theory, and we work up to RSA and how that cryptosystem works, and why factoring is so important. So yeah, you don't have to really have to worry about this. But these things are important.

And the bigger message is that you don't just try a few cases, and if it works, you think it's

done. That's not how the game works in mathematics. You can get an idea of maybe it's true, but doesn't tell you the answer.

All right, let me give you another one. This is another very famous one that probably most of you have heard of. The regions in any map can be colored in four colors so that adjacent regions have different colors. Like a map of the United States-- every state gets a color. If two states share a border, they have different colors so you can distinguish them.

This is known as the four color theorem. And it's very famous in the popular literature. How many people have heard of this theorem before? Yeah, OK. So you've all heard of it.

It has a long history. It was conjectured by somebody named Guthrie in 1853. He's the first person to say this ought to be possible. And there were many false proofs over the ensuing century.

One of the most convincing was a proof using pictures by Kempe in 1879, 26 years later. And this proof was believed for over a decade. Mathematicians thought the proof was right until another mathematician named Heawood found a fatal flaw in the argument.

Now, this proof by Kempe consisted of drawing pictures of what maps have to look like. So he started by saying, a map has to look like one of these types. And he would draw pictures of them. And then he argued that those types that he drew pictures of, it worked for.

Proofs by picture are often very convincing and very wrong. And I'm going to give you one to start lecture next time. It'll be a proof by PowerPoint, which is even worse than proof by picture. And it is compelling. And the point will to be to show you proofs by picture are generally not a good thing. Because your brain just locks in-- oh, that's what it has to look like. And you don't think about other ways that it might look like.

Now, the four color theorem was finally proved by Appel and Haken in 1977, but they had to use a computer to check thousands of cases. Now, this was a little disturbing to mathematicians, because how do they know the computer did the right thing? Your colleague writes a proof on the board. You can check it. But how do you know the computer didn't mess up, or not do some cases?

Now, everybody believes it's true now. But it's unsatisfying.

A few years ago, a 12-page human proof was discovered, but it's not been verified. And

people are very suspicious of it because the proof of the main lemma says, quote, "details of this lemma is left to the reader. See figure seven." That's what the main lemma of the proof is. But people think that maybe there were some good ideas there, but very suspicious proof.

All right, let's do another one, another proposition-- also very famous. Every even integer but 2-- actually, positive integer but 2-- is the sum of two primes. For example, 24 is the sum of 11 and 13, which are prime. Anybody know? Is this true or false, this proposition? Yeah?

AUDIENCE: I wish I knew.

PROFESSOR: [LAUGHS] Yeah, that's right. Me too. Nobody knows if this is true or false. This is called Goldbach's conjecture. It was conjectured by Christian Goldbach in 1742.

This is a really simple proposition. And it's amazing it's not known. In fact, I spent a couple years working on-- I thought, oh, well, this has to be easy enough to prove when I was younger, and didn't get very far. So people still don't know if it's true.

And in fact, it was listed by the *Globe* as one of the great unsolved mysteries. So if you get out this *Globe* article here, one of the hand-- does everybody have this handout? You don't? We'll get it passed out. Somebody missing that handout up over there and over here? All right, if we get those passed out.

Now, it lists the three conjectures. Do you see Goldbach's conjecture there? Now, can anybody point out something that's a little disturbing about what the *Globe* says about Goldbach's conjecture?

AUDIENCE: 9 as a prime number.

PROFESSOR: Yeah, it gives the example. Like, instead of 24 is 11 plus 13, it says 20 is the sum of 9 and 11. Now, if we're allowed to use things like 9 as primes, Goldbach's conjecture's pretty easy to prove is true.

This won't be the last time we get examples from the literature. In fact, we're going to do this a lot, along this theme of, you cannot believe everything you read. Now, the *Globe* is easy pickings, but we'll do some more interesting ones later.

Now, this article lists two other famous conjectures which most people believe to be true-- the Riemann hypothesis after an 1859 paper written by Bernard Riemann suggested that zeros in

an infinite series of numbers known as a zeta function form along a straight line on that complex plane. The hypothesis has been proved to 1.5 billion zeros, not far enough to prove it completely. If they did 1.5 trillion zeros, it wouldn't be far enough to prove it completely, of course.

And then the-- no, actually, the Riemann hypothesis, a couple years ago, somebody credible claimed to have proved it. Proof turned out not to be right. Then there's the Poincare conjecture. Now, this one was finished off. It was proved to be true in 2003 by a Russian named Grigori Perelman.

The conjecture says, roughly speaking, that 3D objects without holes, like no a doughnut, are equivalent to the sphere. They can sort of be deformed into a sphere. This is known to be true in four dimensions and higher, but nobody could prove it for three dimensions until Perelman came along.

Now, there's a bit of a controversy around this guy. He had an 80-page proof, but didn't have all the details. So then other teams of mathematicians got together and wrote 350 pages of details. And then most people believe now that it's right, and that his original proof might not have had all the details, but he had the right structure of the proof.

So he won prizes for this. He won the highest prize in mathematics, the Fields Medal. And just earlier this year, he was awarded the $1 million Millennium Prize.

And there's about six problems or so that if you solve one of them, the Clay Institute gives you a million dollars. And he's the first one to win the million dollars. Now, the guy's a little strange. He rejected the Fields Medal and refused to go to the ceremony where he was being honored. And he's recently rejected the Millennium prize.

And anyway, this area's murky, and we have an expert to explain it all for us on video, which I thought I'd show.

All right, let's do a simpler one here. For all n in Z, n greater than or equal to 2 implies n squared is greater than or equal to 4. Now, Z, we use for the integers. And so that would be 0, 1, minus 1, 2, minus 2, and so forth.

And this symbol here is implies. I In fact, one thing you can notice when you read the text is we use different notation there as the standard than I will use in lecture. And there's lots of ways of doing it. You could have a double arrow, a single arrow. You could write out implies every

time as it's done in the text. And it doesn't really matter which one you want to use as long as you use one of the conventions for implies.

And let me define what implies means. An implication p implies q is said to be true if p is false or q is true, either one. So we can write this down in terms of a truth table as follows. You have the values of p and q. And I'll give the value of p implies q.

If p is true and q is true, what about p implies q? It's true, because q is true in the definition. If p is true and q is false?

AUDIENCE: False.

PROFESSOR: False. P is false. Q is true. True. What about false and false? It's true. Even though this is false, as long as p is false, p implies q is true. So this is important to remember. False implies anything is true, which is a little strange.

There's a famous expression. If pigs could fly, I would be king. Is that true? Sort of. In fact, this statement, pigs fly implies I'm king-- that's true, because pigs don't fly. Doesn't matter whether or not I'm king, which I'm not. Since pigs don't fly, even though that's false, the implication is true.

Now, some of you have worked on these things before. It's second nature. If you haven't, you want to start getting familiar with that. Let's do another example.

What about this proposition? For all integers, n in Z, n greater than or equal to 2-- this is if and only if-- n squared greater than or equal to 4. Is that true? Is n only bigger than 2 if and only if n squared is bigger than 4?

It's false. What's an example of n for which that's false? Negative, all right? So it's false. n equals negative 3, all right? Negative 3 squared is bigger than or equal to 4, but negative 3 is not bigger than or equal to 2.

And in fact this if and only if means you have to have an implication both ways. So you have to check both ways for it. So let's do the truth table-- extend this truth table out here to do the truth table for p if and only if q.

So here are p and q. Is q implies p true for this row? Does true imply true? Yeah. False implies true? That's true. True does not apply false. That's false. And false implies false.

And so now, we can see where p is if and only if q. If they're both true, then it's true here. What about here? Is p true if and only if q is true in this case? No, because p implies q is false, but q implies p is true. So it's false. False here.

I made a mistake there, right? That was true-- oops. And true if and only if true, OK. They're both true, so we're OK.

So p if and only if q is true when they're both true or both false. And that's it. If they're different, then it's not true. The key here is to always check both ways. So if you're asked to prove an if and only if, you have to prove that way, and that way.

We've just done about 15 propositions. Is every sentence a proposition? Yes? No?

AUDIENCE: No.

PROFESSOR: No. What's an example of something that's no a proposition?

AUDIENCE: This statement is false.

PROFESSOR: A what?

AUDIENCE: This statement is false.

PROFESSOR: This statement is false. That's true. Well, it's true it's not a proposition. Because if it were true, it wouldn't be false. And if was false, then it'd be true and you'd have a contradiction. So it's neither true nor false.

What's a more simple example of something that's not a proposition?

AUDIENCE: This is a tissue. Isn't that a [INAUDIBLE]?

PROFESSOR: Ooh. Boy, I would have said that's true in some world. Because yeah, that's a tissue. So it's a true statement.

AUDIENCE: Hello.

PROFESSOR: Hello. That's good. That's neither true or false, yeah. A question. Who are you-- neither true nor false. So not everything is a proposition. But in this course, pretty much everything we deal with will be a proposition.

All right, so that's it for propositions. Any questions on propositions?

Next, we're going to talk about axioms. Now, the good news is that axioms are the same thing, really, as propositions. The only difference is that axioms are propositions that we just assume are true. An axiom is a proposition that is assumed to be true.

There's no proof that an axiom is true. You just assume it because you think it's reasonable. In fact, the word "axiom" comes from Greek. It doesn't mean to be true. It means to think worthy-- something you think is worthy enough to be assumed to be true.

Now, a lot of times, you'll hear people say-- sometimes, we'll even say it to you-- don't make assumptions when you're doing math. No, that's not true. You have to make assumptions when you do math. Otherwise, you can't do anything because you have to start with some axioms.

The key in math is to identify what your assumptions are so people can see them. And the idea is that when you do a proof, anybody who agrees with your assumptions or your axioms can follow your proof. And they have to agree with your conclusion. Now, they might disagree with your axioms, in which case, they're not going to buy your proof.

Now, there are lots of axioms used in math. For example, if a equals b and b equals c, then a equals c. There is no proof of that. But it seems pretty good. And so we just throw it in the bucket of axioms and use it.

Now, axioms can be contradictory in different contexts. Here's a good example. In Euclidean geometry, there's a central axiom that says given a line L and a point p not on L, there is exactly one line through p parallel to L. You all saw this in geometry in middle school, right? You've got a point in a line. There's exactly another line through the point that's parallel to the line.

Now, there's also a field called spherical geometry. And there, you have an axiom that contradicts this. It says, given a line L and a point p not on L, there is no line through p parallel to L on the sphere. There's a field called hyperbolic geometry. And there, there's an axiom that says, given a line L and a point p not on L, there are infinitely many lines through p parallel to L.

So how can this be? Does that mean one of these fields is totally bogus, or two of them are? Because they've got contradictory axes.

That's OK. Just whatever field you're in, state you're axioms. And they do make sense in their various fields. This is planar geometry. This is on the sphere. And this is on hyperbolic geometry. They make sense in those contexts.

So you can have more or less whatever axioms you want. There are sort of two guiding principles to axioms. Axioms should be-- it's called consistent-- and complete. Now, a set of axioms is consistent if no proposition can be proved to be both true and false.

And you can see why that's important. If you spend three weeks proving something's true, and the next day, somebody proves it's also false, I mean, the whole thing was pointless. So it only makes sense if your axioms, as a group, are consistent.

A set of axioms is said to be complete if it can be used to prove every proposition is either true or false. Now, this is desirable because it means-- well, you can solve every problem. Everything is-- you can prove it's true, or you can prove it's false. You can get to the end.

Now, you'd think it shouldn't be too hard to get a set of axioms that satisfies these two basic properties. You're allowed to choose whatever you want, really. Just, you don't want to be creating contradictions. And you want a set that's powerful enough that allows you to prove everything is true or false, one of the two.

Turned out not to be so easy to do this. And in fact, many logicians spent their careers-- famous logicians-- trying to find a set of axioms, just one set, that was consistent and complete. In fact, Russell and Whitehead are probably the two most famous. They spent their entire careers doing this, and they never got there.

Then one day, this guy named Kurt Godel showed up. And in the 1930s, he proved it's not possible that there exists any set of axioms that are both consistent and complete. Now, this discovery devastated the field. It was a huge discovery.

Imagine poor Russell and Whitehead. They spent their entire careers going after this holy grail. Then Kurt shows up and said, hey, guys. There's no grail. It doesn't exist. And that's a little depressing-- pretty bad day when that happened.

Now, it's an amazing result, because it says if you want consistency-- and that's a must-- there will be true facts that you will never be able to prove. We're not going to prove that here. It's proved in a logic course. For example, maybe Goldbach's conjecture is true and it is

impossible to prove.

Now, we're going to try not to assign any of those problems for homework. And in fact, they do exist. It's complicated. You can state a problem that you can't prove is true or false.

And you may be thinking that from time to time. Hey, it's one of those. Remember when your parents told you if you work hard enough, you can do anything? They were wrong.

All right, that's enough for now. And we'll do more of this next time.