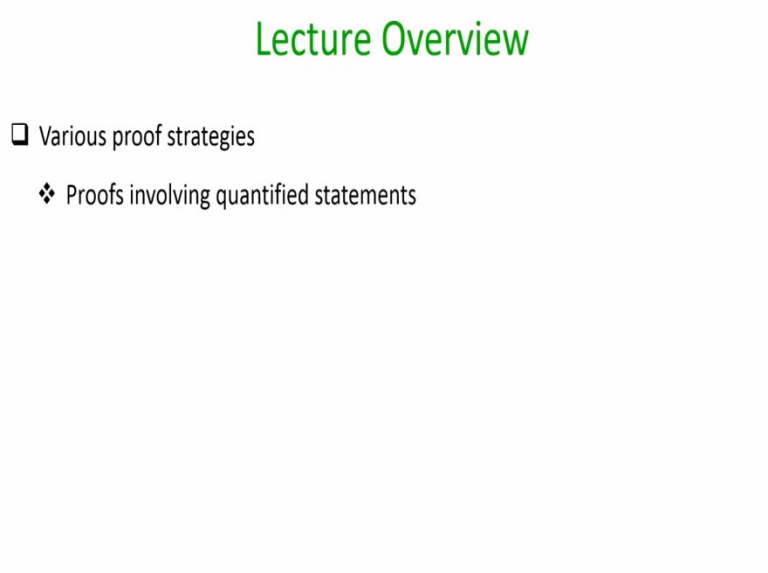
Discrete Mathematics
Prof. Ashish Choudhury
Department of Mathematics and Statistics
International Institute of Information Technology, Bangalore

Lecture -11
Proof Strategies-II

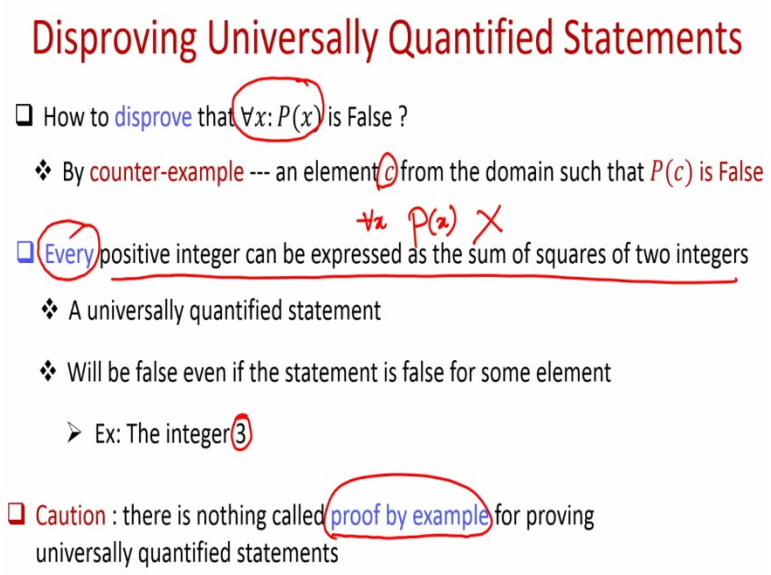
Hello everyone, welcome to the second part of proof strategies.

(Refer Slide Time: 00:26)



In this lecture we will continue our discussion on the proof strategies that we started in the previous lecture.

(Refer Slide Time: 00:32)



We will start with how to disprove a universally quantified statement. So till now we were seeing various proof methods, where we wanted to prove universal quantified statements. But sometimes we also encounter statements where we want to prove that a universal statement, universally quantified statement, is not true. To disprove that a universally quantified statement is not true we have to give what we call as a counterexample.

And, by counterexample we mean some element c from the domain such that the statement P is not true for the element c, because if the statement P is not true for the element c. Then the universal quantification for all x, P(x) will turn out to be false. So, very simple example of this is if I make a statement that every positive integer can be expressed as the sum of squares of 2 integers. So this property is my property P and I am making this statement for every x.

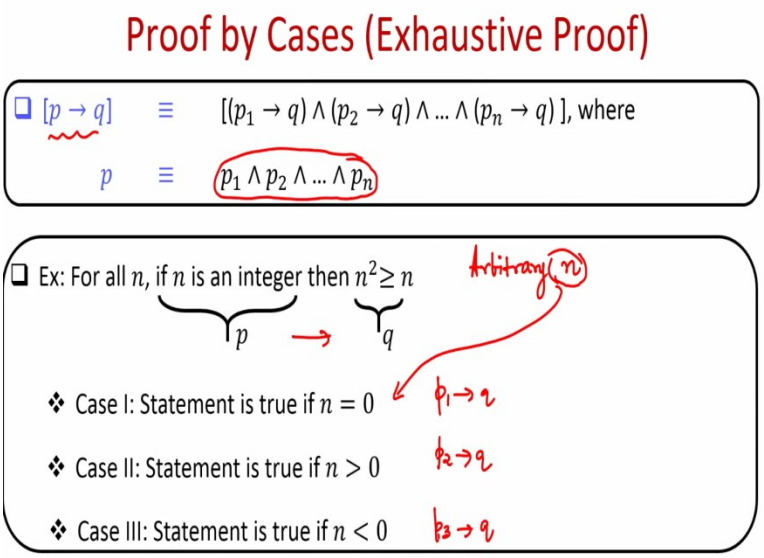
So, now I have to verify whether the statement P is true for every integer x or not. Even if I can find one integer for which this property is not true, I can say that ∀ x, P(x) is false here and a very simple counterexample is 3 here, you can check that 3 can never be expressed as a sum of squares of 2 integers. You can never do that. So that is how we disprove universally quantified statement.

However, I would like to stress here that there is nothing called proof by example for proving universally quantified statements. If you want to prove that your statement P is true for every

element in the domain, then you cannot say that okay, I am showing it for some x, where x is explicitly chosen by you, it is not arbitrary. You are not choosing your x arbitrary, you are just taking your x specifically and that is an example for you.

And you show that a property P is true for that specific x and then you happily conclude that P is true for every x in the domain. What if there is some bad x which you have not verified for the property P. So that is why when we try to prove universally quantified statement the witness c is chosen arbitrarily, it is not chosen in some specific well defined way.

(Refer Slide Time: 03:06)



There is another proof mechanism which is called proof by cases. This is also called exhaustive proof. So if you want to prove an implication of the form p →q, where p and q are propositions, are propositions and if you are proposition P can be decomposed into conjunction of various other propositions say n propositions, then p → q is logically equivalent to p_1 → q, conjunction p_2 → q and so on.

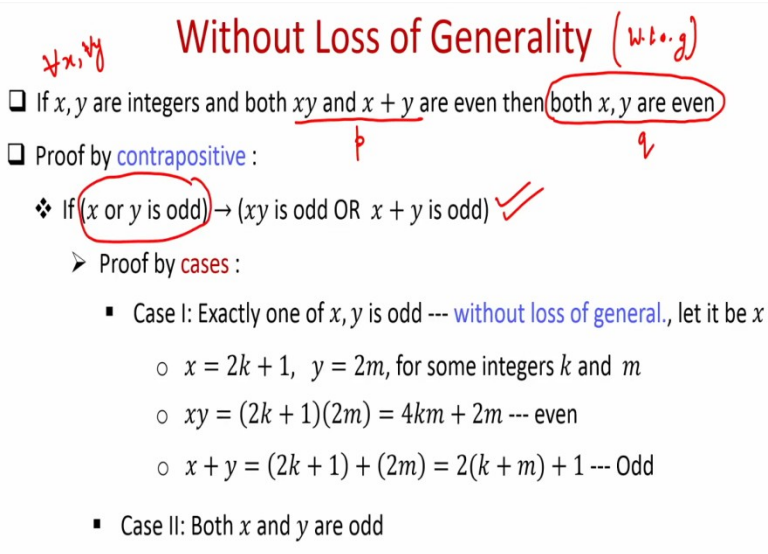
That means here p_1, p_2, p_n are the various cases for your proposition p and your goal was to prove p → q. So to do that, you show that for various cases for p that sub case implies q is true. That is why it is the essence of the proof mechanism. So for instance, if I want to prove a statement that ∀ n, if n is an integer, then $n^2 \geq n$. This is a universally quantified statement.

And now if I apply the universal generalization, you will be choosing an arbitrary n and you will be trying to prove that this property is true for that arbitrarily chosen integer. But now that arbitrarily chosen integer can be positive, it can be negative, it can be 0. You have 3 possible cases right for this arbitrarily chosen n and that is why you split the proof into three cases and you show that p → q is true for any of those three cases does not matter which case you are in.

So if you take the case n equal to 0 the statement is true, namely p → q is true. If you take the case when your arbitrarily chosen n is positive, then also this statement p → q is true and if your arbitrarily chosen n is negative, then you show that in that case also this p → q is true and since these are the three possible cases for your arbitrarily chosen n and you have chosen that p_1 → q is true p_2 → q is true and p_3 → q is true.

And there are only three possible divisions or cases for your p, you can conclude that p → q is true. So that is your proof by cases method.

(Refer Slide Time: 05:30)



There is also something called without loss of generality, which we very often encounter while writing the proof. In short form they call it as w.l.o.g. So let me demonstrate we have what exactly I mean by without loss of generality. So imagine I want to prove that if x and y are integers and both x, y and x + y are even, then x and y are both even. That is a statement I am making and again, this is a statement involving for all x for all y.

Because; I am making a statement for all integers x and all integers y. So, let me try to prove it by contrapositive. So the contrapositive means a negation of the condition appearing after then. So I wanted to prove both x and y are even, so, that is my q part. So negation of q will be either x is odd or y is odd. Because both means AND negation of AND means OR and in the same way this is my p, so negation of p will be x, y is odd OR x + y is odd.

So this is what I want to prove now and now I can apply proof by cases because I am taking arbitrary x and arbitrary y here and my premise is that either x is odd or y is odd. So now I have three possible cases. Case 1, when x is odd y is even, so let us prove it for that part. So since x is an arbitrary odd number, I can write it in the form x equal to 2k + 1, I can say y is equal to 2 times of m because y is even.

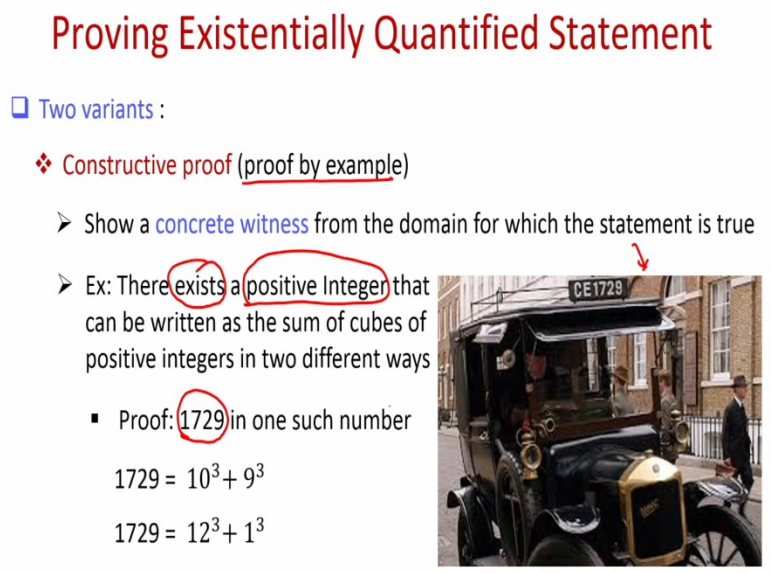
Then x times y turns out to be even, but x + y turns out to be odd that means the statement turns out to be correct. So this is case 1 for the premise x or y is, one of x or y is odd. The Case 2 could be when x is even, y is odd that also satisfies my premise but it turns out that I do not need to explicitly write a proof for Case 2, because this case will be symmetric to your Case number 1. Why it is symmetric? Because for Case 1 you chose x to be arbitrary and y to be arbitrary.

They were not specific values and even for Case 2 your x is arbitrary and your y is arbitrary that means whatever argument you gave for Case 1, the same argument is applicable as it is for case 2 as well. So there is no need to separately write down these 3 statements for case number 2. You just have to swap the rules of x and y for whatever proof you have given for Case number 1 and that is possible that subsumed for in case 1 because x and y were arbitrarily chosen.

So that is why there are not 3 cases for this premise instead, there are two cases only. Case 1 when exactly 1 of x or y is odd. This is different from a previous case 1, my previous case 1, I was explicitly taking the cases x odd, y even, x even, y odd and my third case would have been both x and y are odd. But what I am doing now is I am clubbing both case 1 and case 2 into one new case 1, where I say that exactly 1 of x and y is odd which one I do not know.

It could be either x or either y and that is why I can say that I do not know which one of x and y is odd without loss of generality. Let it be x and for that particular case this argument is given. This argument automatically subsumes the case when y is odd as well and now my second case will be when both x and y are odd. So these will be now the two subcases for my premise x or y is odd. There will not be three separate cases because two of the sub cases are subsumed by one sub case here.

(Refer Slide Time: 09:47)



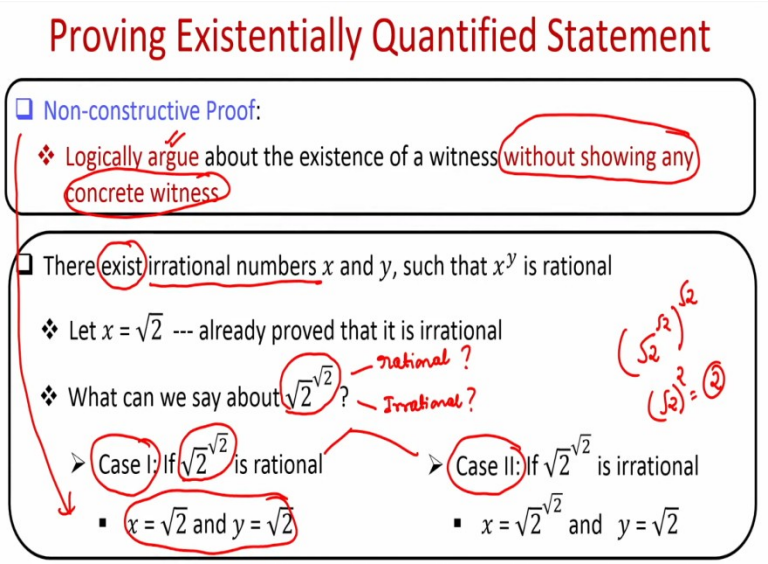
We also need proof mechanisms for proving existential quantified statements and there are two variants for that. Variant one is called constructive proof where we give a specific example specific witness and show that specific witness satisfies my conditional property. Because when I want to prove an existentially quantified statement, I have to show that a statement is true for at least one value in the domain.

There might be multiple values, but I just have to show one value for which the statement is true that I can do by giving a constructive proof by showing an explicit example. So for instance here is an example of existentially quantified statement that says that there exists a positive integer that can be written as the sum of cubes of positive integers in two different ways. So there might be several such positive integers which can satisfy this positive property.

My goal is to show whether at least one such integer exist or not and indeed 1729 is one such number of course, as I said there can be multiple such integers and you can check that 1729 can be written as the summation of 10^3 and 9^3, as well as the summation of 12^3 and 1^3. That means it can be expressed as a sum of cubes of two numbers in two different ways.

If you are wondering why I am showing this car here, some of you might know the famous story about this number 1729, so this is also called Ramanujan Number. So the story goes says that Ramanujan and Mathematician Hardy were travelling in a car in London and there was this car with number 1729 in front of their car. So Hardy said that is nothing interesting about this number 1729. But the great Ramanujan said no it is an interesting number, because it can be expressed as the sum of cubes of two numbers in two different ways.

(Refer Slide Time: 11:54)



So that is one way of proving existentially quantified statements, another way of proving existential quantified statements is what we call as non constructive proof and here we do not show any concrete example or witness from the domain for which the statement is true. We do not do that, but we logically argue that definitely at least one element from the domain exists for which the property is true.

So let me demonstrate this proof mechanism by this statement I want to prove that there exists irrational numbers x and y. Such that x^y is rational, again there might be multiple x and multiple

y satisfying this condition, but I have to show the existence of at least one such x, y pair. It turns out that I cannot explicitly show that x, y pair, but I can guarantee I can logically argue that definitely such x, y per exist. How?

So consider the number x equal to $\sqrt{2}$. We already proved that it is irrational. We proved it in our previous lecture using the proof by contradiction method, we assumed x to be, we assumed $\sqrt{2}$ to be rational and then we came to the conclusion that both r and negation r exist where r is some statement. So we already proved that $\sqrt{2}$ is irrational. Now, what can you say about the number $(\sqrt{2})^{(\sqrt{2})}$.

There can be only 2 possibilities either this is rational or this is irrational. Only 2 possibilities, we cannot have any third possibility. So, these are the two possible cases. Now if $\sqrt{2}$, raised to power $\sqrt{2}$ is rational then I got my witness x, y. My witness in that case will be x to be $\sqrt{2}$ and y to be $\sqrt{2}$. Whereas, if $\sqrt{2}$ to the power $\sqrt{2}$ is irrational then my x y candidate is the following I will take x to be $\sqrt{2}$ to the power $\sqrt{2}$ and y to be $\sqrt{2}$.

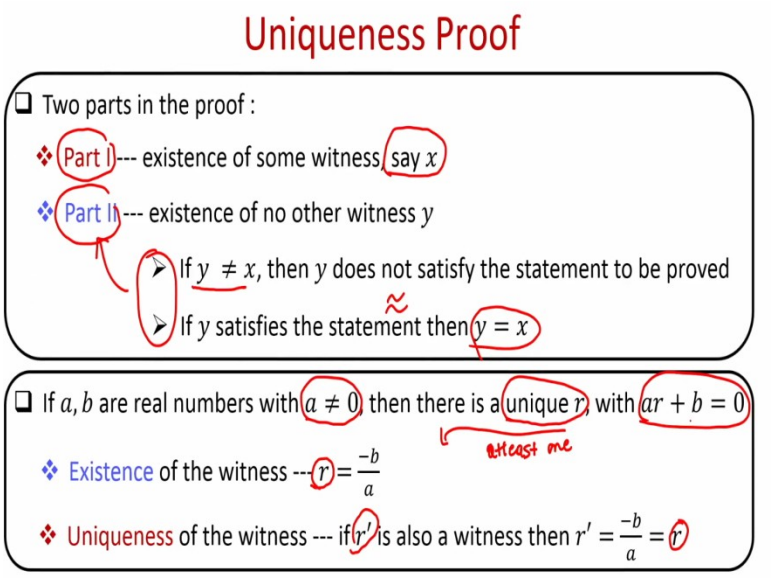
Because if $\sqrt{2}$ to the power $\sqrt{2}$ is irrational and I raise it to again power $\sqrt{2}$, then this is equivalent to saying $(\sqrt{2})^2$, which is 2 and 2 is rational. Now you might be wondering how it constitutes a proof, we do not know for surety whether it is case 1 or whether it is case 2 which is true, we cannot verify whether $\sqrt{2}$ power $\sqrt{2}$ is rational or irrational but what we are logically arguing is that either it will be this case or this case.

And, it does not matter whether it is case 1 which is true or it does not matter whether it is case 2 is true in both cases I can show you an x,y pair satisfying the conditions that I am stating in this theorem statement and that is why this is a non-constructive proof. You cannot say that my x and y is always $\sqrt{2}$ and $\sqrt{2}$. We do not know or you cannot say that my x is $\sqrt{2}$ power $\sqrt{2}$ and y is $\sqrt{2}$.

It depends whether I am case 1 or case 2, but I do not know whether it is case 1 which is always true or whether this case 2 which is always true. But I know definitely logically that one of them is true. So that is what we do in non-constructive proof method, we do not give you the explicit

witness, but we logically argue that the statement that we are making is true for some witness in the domain.

(Refer Slide Time: 15:39)



We also encounter proof statements where we have to prove the uniqueness of something and namely we have to show the uniqueness of some element which satisfies a given property of the theorem statement, and such proofs involve two parts. The part 1 will be the existence of some witness, say x that means we have to show that definitely the property that is mentioned in the theorem statement holds for some x in the domain.

And the second part is we have to show that apart from x there is no other witness y which also has the same property mentioned in the theorem statement. This is equivalent to saying that if you had a different witness y from x, where x has already satisfied the property p then y cannot satisfy the statement to be proved or equivalently if y satisfies the same property, which is given in the statement then definitely y equal to x.

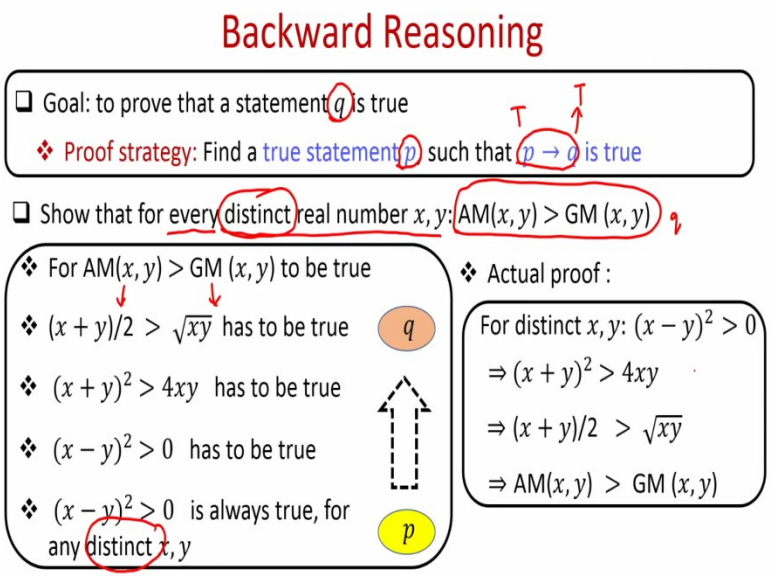
These are equivalent and both of them represent this part 2. This is something similar to what we did in the lecture where we represented English statements by predicates, there we represented a statement of the form that every person has exactly one best friend. So there we first logically represented that a person has at least one best friend and we negated in the same expression that apart from that friend he cannot have a second best friend.

So that is the part 2 here. Part 1 is you show that some witness is there; part 2 you show that no other witness is there. So this is an example of a statement where you have to show the uniqueness of something. The statement is if a and b are real numbers again, this is a universally quantified statement because we are making the statement for all real numbers a and b. The statement is if a is not equal to 0 then there is a unique r such that the condition a times r + b equal to 0 holds.

So part 1 of the proof will be we have to show that, at least one r is there which satisfies this property. That is a part 1 of the proof and indeed an r satisfying this property is minus b over a and minus b over a is well defined, because a is not equal to 0. That is why this condition a is not equal to 0 is important. If a is equal to 0, then this property that a times r + b equal to 0 may not hold.

Now, we have to argue that apart from this value of r namely minus b over a, there is no other integer value possible satisfying the same condition and this simply follows from the fact that if you have another witness r', which also satisfies the same property. Then r' also will be minus b over a and minus b over a is nothing but r; that means you cannot have anything different from minus b over a which can satisfy this condition a times r + b equal to 0. So this is an example of uniqueness proof.

(Refer Slide Time: 18:50)



We have another proof mechanism called backward reasoning and this is an interesting proof mechanism. So imagine your goal is to prove a statement q to be true. The proof strategy that is involved here is instead of proving q to be true; we will try to find out statement p instead, which is true. Such that p → q is true. So we will not be proving q here, our goal will be to instead find this true statement p.

Such that p → q is true and if p → q is true and p is true that is possible then that is possible only if q is true, because if we are showing p to be true and simultaneously implies q to be true, then that is possible only if q is also true that is a proof mechanism here. So let me demonstrate this proof mechanism by this theorem statement by proving this theorem statement we want to prove that for every distinct real numbers x and y their arithmetic mean is always greater than the geometric mean and again this is a universally quantified statement. What we will do is instead of proving it for every x and y we will try to prove this property for an arbitrary x and arbitrary y that is the statement q. My statement q is that for an arbitrarily chosen x and y arithmetic mean is greater than geometric mean, that is what I want to prove.

So our goal will be to find the true statement p involving this arbitrary x and y, such that p → q is true. So here is how we find the statement p. What we do is we keep on going backward starting with q, till we arrive at a statement p which is true and then we will try to see whether we

can come back all the way from that p to our goal q. So as I am saying that we have to go backward.

So we argue that in order that arithmetic mean is greater than geometric mean the condition x + y over 2 should be greater than the square root of x + y why? Because, this is your definition of arithmetic mean and geometric mean and this is the statement q, which you want to prove. Well this will be true, provided the square of x + y is greater than 4 times x times y and for this to happen, the square of x - y should be greater than 0.

But this is always true because you are given that your arbitrary x and y are distinct here. That is what is the condition here and for any arbitrary distinct x and y, it does not matter whether x is greater than y or y is greater than x. The square of their difference will always be positive which is a true statement and this is the statement p which we are interested to find a true statement p which is always true.

Now the actual proof in the backward reasoning will be to reverse this argument and show that starting with p, assuming p to be true, you can come all the way to the conclusion q. That will complete the proof; until and unless you do not do this backward reasoning, your proof is not complete you have shown p to be true assuming, q to be true. That is not what you want to prove you wanted to prove the truth of statement q. So the actual proof will be as follows.

We start with the true statement p, we know that what all distinct x, y the square of their difference is always positive, from that we can come to the conclusion that the square of their sum is greater than 4 times xy. From that we can come to the conclusion that x + y over 2 is greater than the root of xy and from that I can come to the conclusion that arithmetic mean, is greater than the geometric mean.

So that brings me to the end of this lecture we have seen in this lecture some other proof mechanisms or indirect proof mechanisms and we have seen proof mechanisms for proving existential quantified statement namely the constructive method and the non-constructive methods and we also saw the backward receiving method. So we have seen lots of interesting

proof mechanisms, we will be encountering all of them in various forms throughout this course. Thank you.