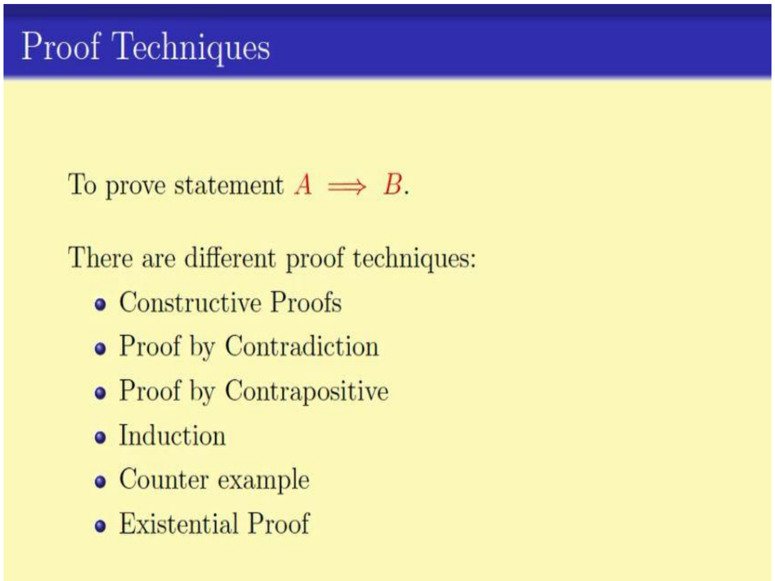
Discrete Mathematics
Prof. Sourav Chakraborty
Department of Mathematics
Indian Institute of Technology – Madras

Lecture - 07
Proof Technique (Direct Proof)

Welcome to the 7th video lecture in this discrete mathematics course. In this video, we will continue with our study of proof techniques. We will look at some of the problems and some new techniques of solving them.

(Refer Slide Time: 00:17)



Proof Techniques

To prove statement $A \implies B$.

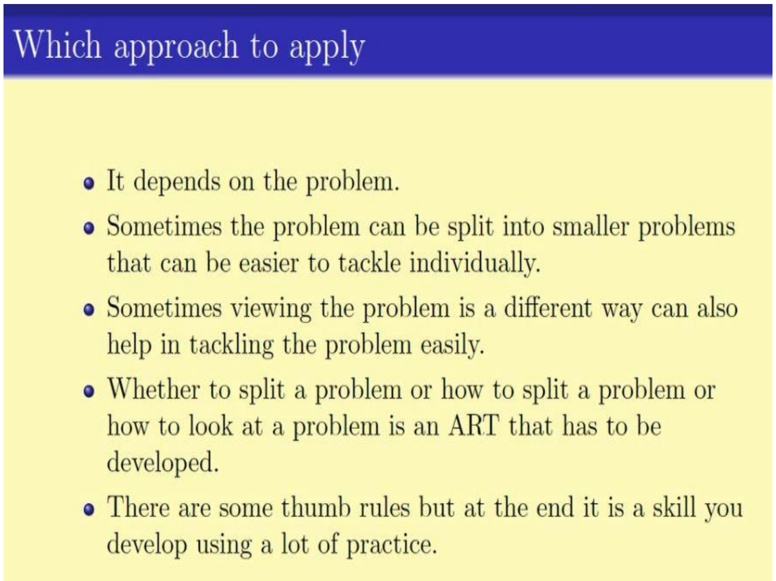
There are different proof techniques:

- Constructive Proofs
- Proof by Contradiction
- Proof by Contrapositive
- Induction
- Counter example
- Existential Proof

So far we have seen that a theorem can be represented as A implies B where A is the set of assumptions and B is the detection. There are different techniques, proof techniques for attacking this problem namely say constructive proofs, proof by contradiction, proof by contrapositive, induction, counter example, existential proof and so on. In this course we will be going over all these proof techniques one by one and doing each of these proof techniques carefully.

Now we will be doing lot of problems and many of the problems will require some of the proof techniques or in other words some of the proof techniques will make some of the problems easier.

(Refer Slide Time: 01:16)



Which approach to apply

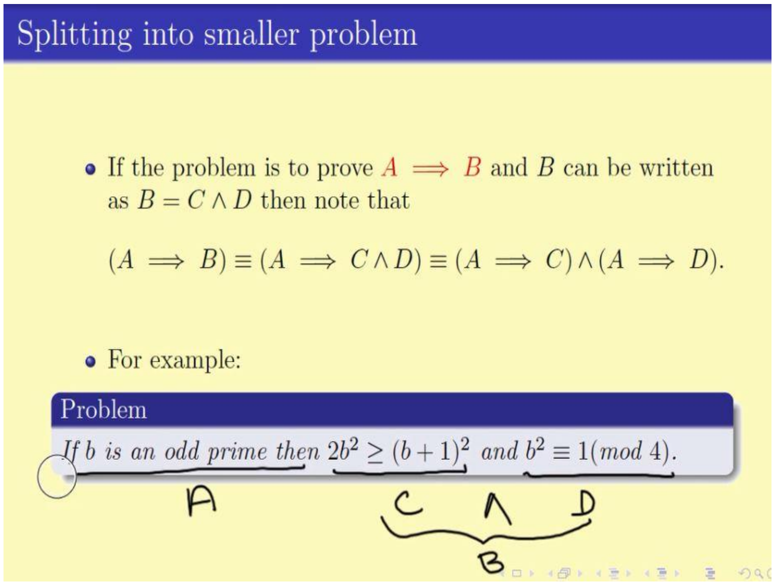
- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.
- Sometimes viewing the problem is a different way can also help in tackling the problem easily.
- Whether to split a problem or how to split a problem or how to look at a problem is an ART that has to be developed.
- There are some thumb rules but at the end it is a skill you develop using a lot of practice.

But the main question, which will be asked will be that which approach to apply. In other words, which problem should be used, which proof technique should be used to solve which problem? Now this depends on the problem. Some problems can be split into smaller problems and that can be tackled easily. In other words, smaller problems can be tackled easily. Some problems can be viewed in a different way and that can help in tackling the problems.

But which problem to split and how to split the problem or how to view this problem is an art in itself that cannot be exactly taught, it has to be learnt by you by doing a lot of problems. You will get a lot of exercises. We can in this course tell you about the various proof techniques, give you some thumb rules, like this kind of problems. For this kind of problems mean this proof technique is an easier technique and so on.

But at the end it would be your skill and your creative mind and that has to be developed with lot of practice for solving these problems and deciding which proof techniques will apply.

(Refer Slide Time: 02:53)



Splitting into smaller problem

- If the problem is to prove $A \implies B$ and B can be written as $B = C \wedge D$ then note that

$$(A \implies B) \equiv (A \implies C \wedge D) \equiv (A \implies C) \wedge (A \implies D).$$

- For example:

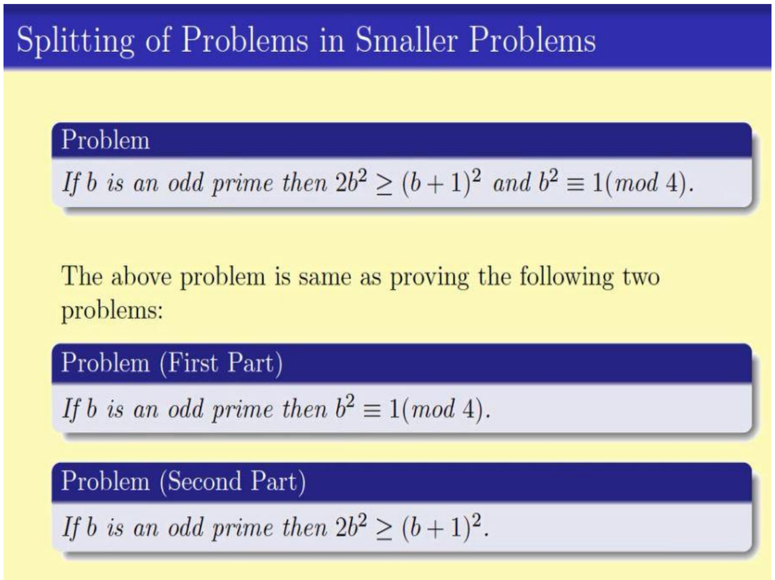
Problem

$$\underbrace{\textit{If } b \textit{ is an odd prime then}}_{A}\ \underbrace{\underbrace{2b^2 \geq (b+1)^2}_{C}\ \underbrace{\textit{and}}_{\wedge}\ \underbrace{b^2 \equiv 1(mod\ 4)}_{D}}_{B}.$$

So to start with, let us consider one of the most easiest case, this is something we did in the last video namely say if I have to prove A implies B and B can be written as C and D, B can be split into two parts. Then, A implies B is same as proving A implies C and A implies D. So, this can help us in splitting this problem. So, for example we were looking at this problem, which says that if b is an odd prime then 2 b square is greater than or equal to b + 1 whole square and b square is congruent to 1 (mod 4).

In this problem, b is an odd prime. This is of course A and b Square is greater than or equal to b + 1 whole square and b square congruent to 1 (mod 4), you can clearly see that this is the C, this is the D, here is an AND and this whole thing together is the B. So in other word, A implies B can be split up as A implies C and A implies D.

(Refer Slide Time: 04:36)



Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ *and* $b^2 \equiv 1(mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

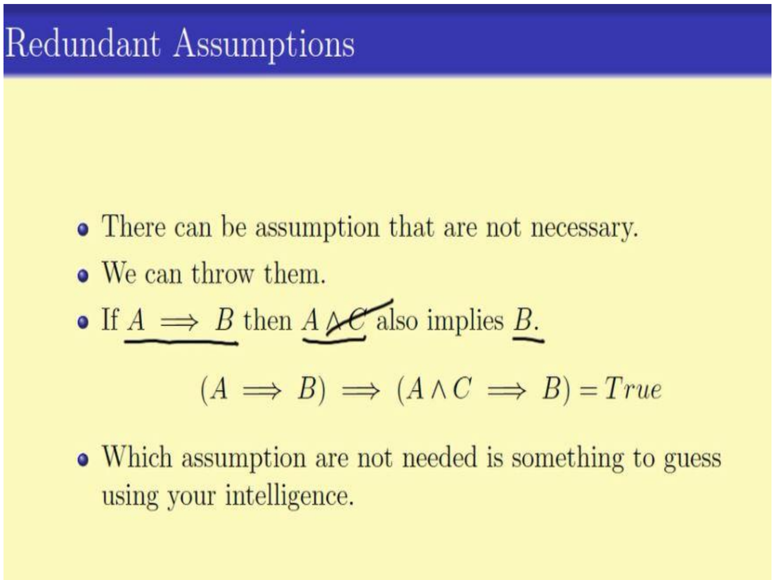
If b is an odd prime then $b^2 \equiv 1(mod\ 4)$.

Problem (Second Part)

If b is an odd prime then $2b^2 \geq (b+1)^2$.

Thus this problem can be split up into these two parts namely First part, if b is an odd prime then b Square congruent to 1 (mod 4) and Secondly, if b is an odd prime then b Square, 2 b Square is strictly, is greater than or equal to b + 1 whole square.

(Refer Slide Time: 05:08)



Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.
- If $\underline{A \implies B}$ then $\underline{A \cancel{\wedge C}}$ also implies $\underline{B}$.

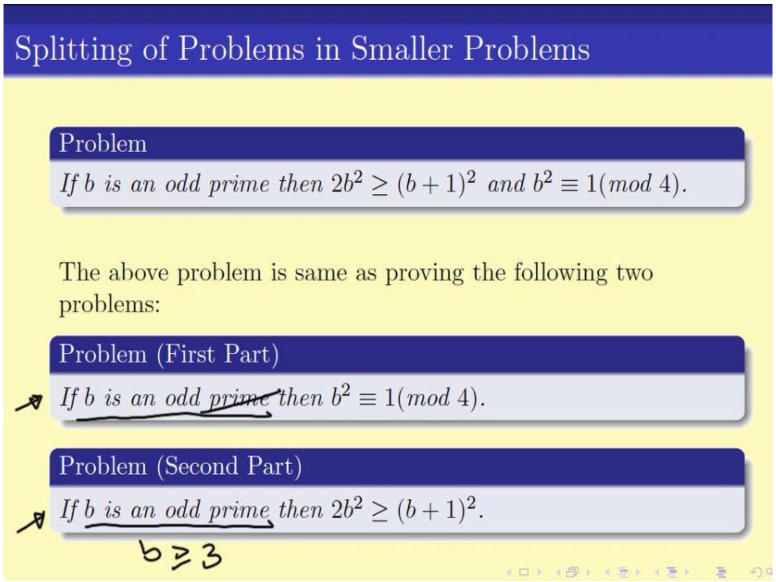
$$(A \implies B) \implies (A \wedge C \implies B) = True$$

- Which assumption are not needed is something to guess using your intelligence.

Now, there can be lot of redundant assumptions also and those can be cleaned up. In other words, there can be many assumptions that are not necessary that only makes the problem more complicated, so if we can throw them, that will also help us in simplifying the problem. So in other words, if I have to prove A AND C implies B. And but I can already prove A implies B that means C is a redundant assumption.

So in other words, A implies B is good enough to prove A AND C implies B. So, one need to find out the assumptions, which are redundant and throw them. But quick assumption are not needed, is something that only can come in practice and all by using your intelligence.

(Refer Slide Time: 06:21)



Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ *and* $b^2 \equiv 1(mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

If b is an odd ~~prime~~ then $b^2 \equiv 1(mod\ 4)$.

Problem (Second Part)

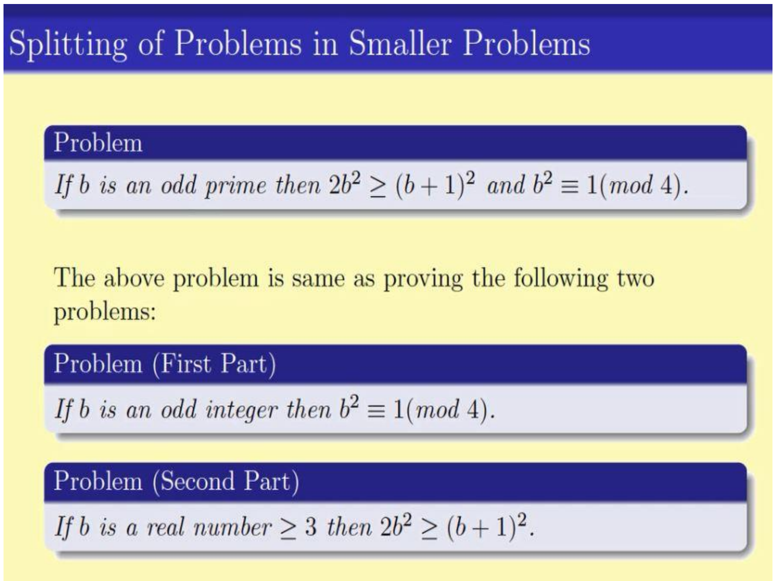
If b is an odd prime then $2b^2 \geq (b+1)^2$.

$b \geq 3$

For example, the problem that we are looking at already, we had split up into this two problems first part and second part. And look at the first part, the first part says that if b is an odd Prime then b Square is congruent to 1 (mod 4). We had discussed it in the last video that what property of odd Prime do we need here. And as we, as I told last class, last video all we need here is that b is an odd number. So the prime is not necessary. Be any odd number that b square congruent 1 mod 4.

Taken this second part, value of proof that 2 b Square is greater than or equal to b + 1 whole square, what is the property of the odd prime do we need. We will only need the fact that b is greater than or equal to 3. Well, if it is an odd prime it has to be greater than or equal to 3. So namely, the fact that the prime or it is an odd and so on what is written as assumption, if I am guessing? So depending on the problem, we might have to throw away some of the redundant assumptions.

(Refer Slide Time: 07:50)



Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1(mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

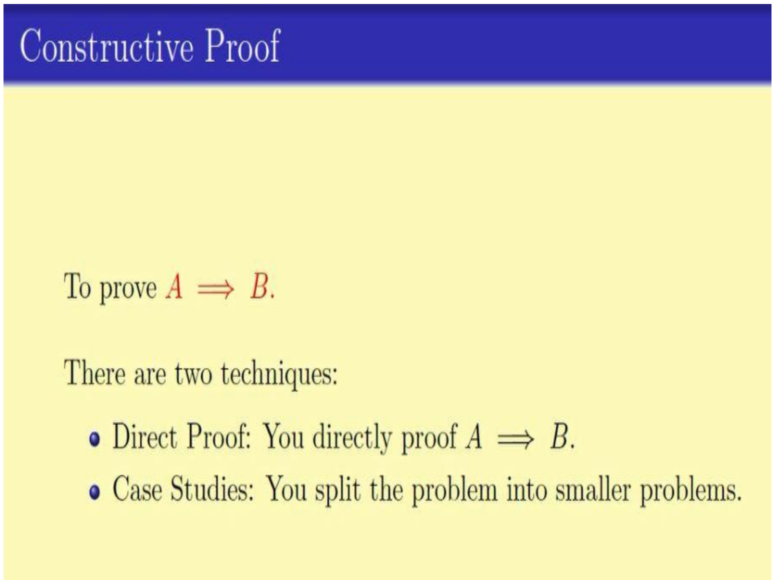
If b is an odd integer then $b^2 \equiv 1(mod\ 4)$.

Problem (Second Part)

If b is a real number ≥ 3 then $2b^2 \geq (b+1)^2$.

So in other words, this problem can be written as this problem. So, these are good enough problems. We mean this problem implies the other problem. Namely if b is an odd integer, then b Square is congruent to 1 mod 4 and the other one if b is the real number greater than, strictly greater than 3, then 2 b Square is greater than b + 1 whole square. In this video lecture, we will be solving these two problems. We will solve these two problems using what is known as the constructive proof.

(Refer Slide Time: 08:28)



Constructive Proof

To prove $A \implies B$.

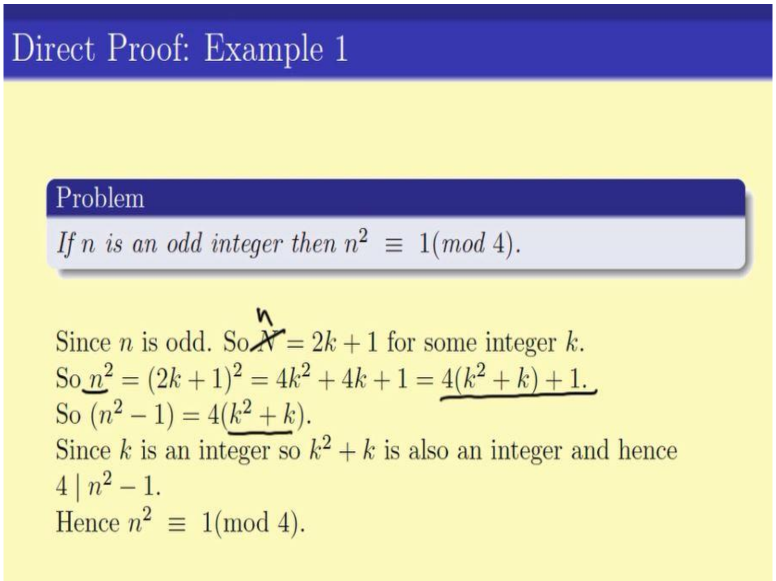
There are two techniques:

- Direct Proof: You directly proof $A \implies B$.
- Case Studies: You split the problem into smaller problems.

Now, what is the constructive proof? A constructive proof, of course, it proves this A implies B. But the idea is that we don't rephrase this problem in any other way. We just start with A and end with B or something similar of that. There are 2 cases, of course number one is the Direct proof, I will start from A and end with B and the second case, which is the case study, where we split the problems depending on A.

Now in this particular video, we will be using this direct proof technique to solve both the problems. We will be doing case study problems in the next 2 videos in this week. And in the next week, we will be going into more complicated non constructive proofs, which are like proof by contradiction or contrapositive or induction so on. Now, let us start with the first problem.

(Refer Slide Time: 09:37)



Direct Proof: Example 1

Problem

If n is an odd integer then $n^2 \equiv 1(\mathit{mod}\ 4)$.

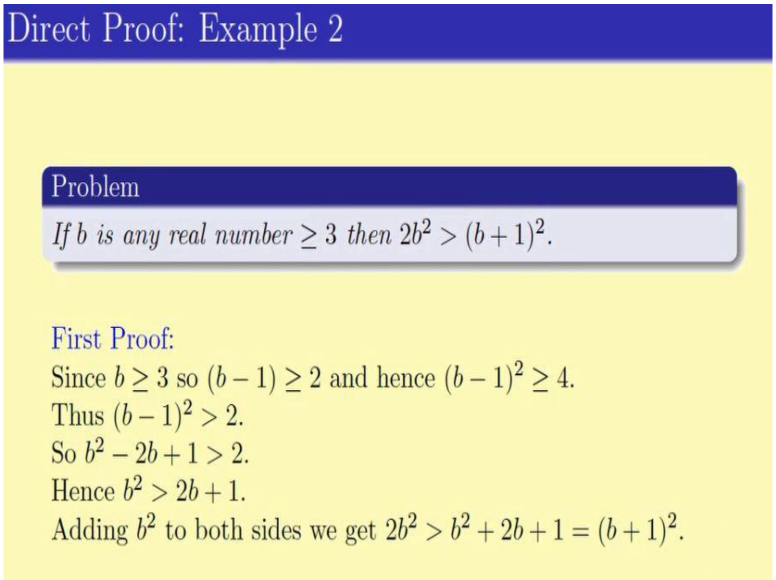
Since n is odd. So $\overset{n}{\cancel{N}} = 2k + 1$ for some integer k.
So $\underline{n}^2 = (2k+1)^2 = 4k^2 + 4k + 1 = \underline{4(k^2+k)+1.}$
So $(n^2 - 1) = 4(\underline{k^2 + k})$.
Since k is an integer so $k^2 + k$ is also an integer and hence
$4 \mid n^2 - 1$.
Hence $n^2 \equiv 1(\text{mod } 4)$.

In the first problem, it is told that n is an odd integer, then prove that n Square is congruent to 1 (mod 4). Now, if n is an odd integer that means N is equals to 2 k + 1. There is a mistake this will be small n, so small n should be is equals to 2 k + 1 for some integer k. Right. Let us have a definition of oddness. If that is the case, then what is n square? n square is (2 k + 1) whole square, which is 4 k Square + 4 k + 1, which I just collect it as 4 times (k Square + k) + 1.

So, by rearranging the numbers we get n Square - 1. So by taking this n Square and this 4 k Square + 1, we get n Square - 1 is equal to 4 times (k Square + k). Now let us look at this number (k Square + k). Since k is an integer, so k Square is an integer, k is an integer. So for k Square + k is also an integer and hence this expression means that n Square - 1 is 4 times some integer or in other words n Square - 1 is divisible by 4, which is just what we mean by when we write the notation n Square is congruent to 1 (mod 4).

Now, this is the pretty simple direct proof, we started with the assumption that n is an odd integer, we worked our way through, we did the obvious things, there was an n Square sitting there, so we had to Square the n which was, since n was odd it was 2 k + 1 and we continue like that and (()) (11:39). Now things, which were not be so easy in some times. Things can be a bit more tricky.

(Refer Slide Time: 11:53)



Direct Proof: Example 2

Problem

If b is any real number ≥ 3 *then* $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.

Thus $(b-1)^2 > 2$.

So $b^2 - 2b + 1 > 2$.

Hence $b^2 > 2b + 1$.

Adding b^2 to both sides we get $2b^2 > b^2 + 2b + 1 = (b+1)^2$.

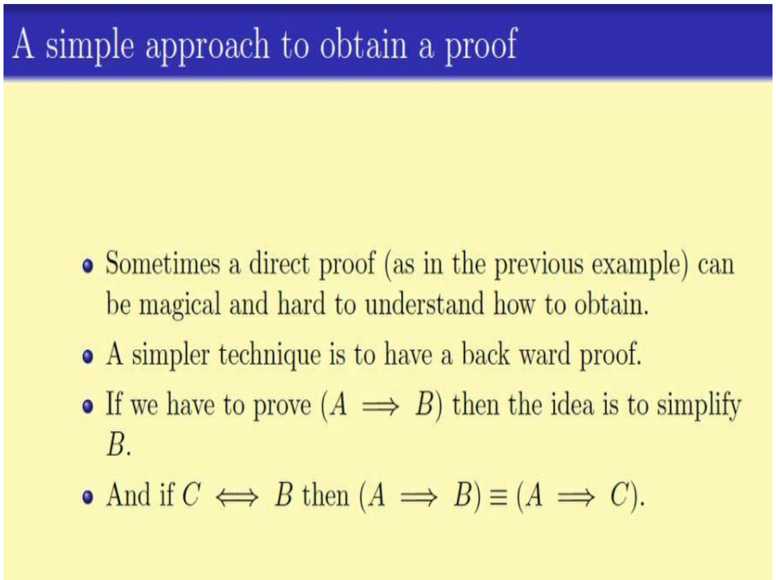
For example, let us consider the following the other example that was there namely if b is an any real number greater than or equal to 3, then 2 b square is strictly greater than (b + 1) whole square. So, how do you prove it? So let me first give you the one proof, the first proof or the First proof. Let us start with, since b is greater than or equal to 3, so b - 1 is greater than or equal to 2, by squaring both, sides we get b - 1 whole square is greater than or equal to 4.

And this 4 is strictly greater than 2, we can write b - 1 whole square is strictly greater than 2. Now let us try to open up (b – 1) whole square, we get b Square - 2 b + 1 is greater than, strictly greater than 2. Quickly, if I rearrange it correctly, by taking the 2b + 1 in the other side, I get b Square is greater than 2 b + 1. This + 1 and + 2 cancels out and leaves plus one behind. So, I have b Square greater than or strictly greater than 2 b + 1.

And, now if I add b Square to both sides, I get 2 b square is greater than, strictly greater than b square + 2 b + 1, which is nothing but (b + 1) whole square. So, now this is also a direct proof. The problem is that this direct proof must have looked a bit magical to you. In the other words, you started from the fact that b is greater than 3, then will be the lot of tricky things.

For example, why did we write it in the form of b - 1 greater than or equal to 2? Why did we even squared it? Why did we do these weird calculations of splitting up and all those things? Or in other words the most important things are why did we consider (b – 1) whole Square. Now these can indeed be pretty tricky and they can be magical.

(Refer Slide Time: 14:32)



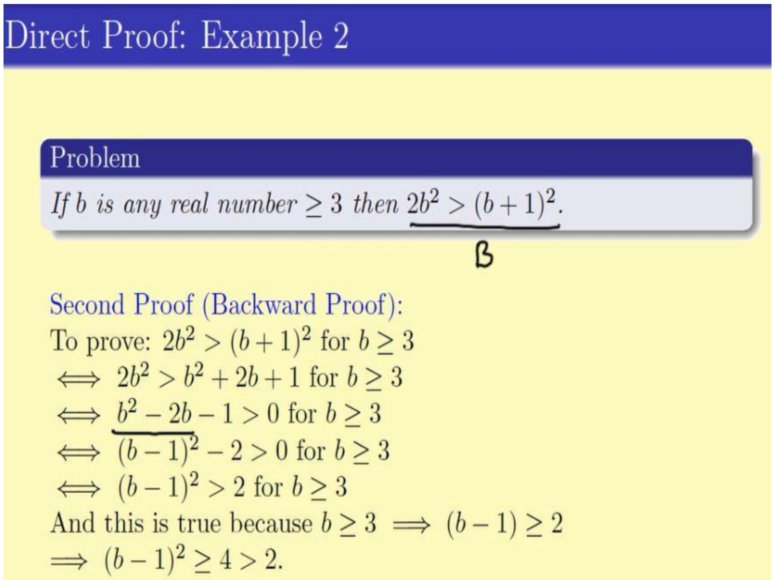
A simple approach to obtain a proof

- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a back ward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.
- And if $C \iff B$ then $(A \implies B) \equiv (A \implies C)$.

Thus, sometimes a direct proof can be magical and hard to understand how to obtain. It is not the problem the proof itself was hard, it is just the proof was magical. Proof started from somewhere and ended somewhere and you would think if I have to, if I am ought to solve these problems in an exam, how will I do it? And here you must have to face the similar question in your mind, in your high school or in other math courses.

Now, there is a simpler technique to attempt this problem. This is called the backward proof. Or in other words, it starts from the backward and go ahead. So here that means that if I ask to prove A implies B, the idea is to simplify B and get something simple. And if I, in the end I can prove that B is equivalent to C or in other words B and C are same then, A implies B proving that same as proving A implies C and which can be easy if I manage to put C to B. C (()) (15:50) easy number (()) (15:52). So let us look at this problem again. How do we apply this backward proof to this technique?

(Refer Slide Time: 16:00)



Direct Proof: Example 2

Problem

If b is any real number ≥ 3 *then* $\underbrace{2b^2 > (b+1)^2}_{B}$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff \underline{b^2 - 2b} - 1 > 0$ for $b \geq 3$

$\iff (b-1)^2 - 2 > 0$ for $b \geq 3$

$\iff (b-1)^2 > 2$ for $b \geq 3$

And this is true because $b \geq 3 \implies (b-1) \geq 2$

$\implies (b-1)^2 \geq 4 > 2$.

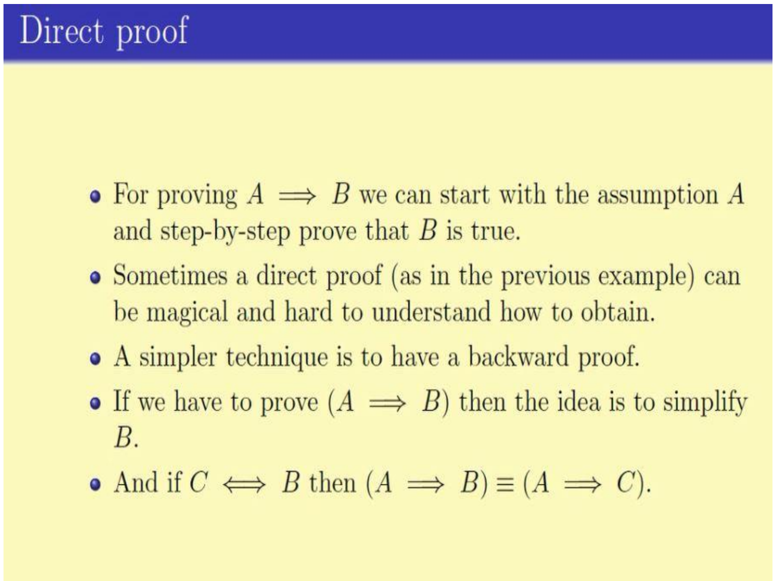
So if b is an any real number greater than or equal to 3, then 2 b Square is strictly greater than b + 1 whole Square. So, the back ward proof of it would be to play around with the B. So this the B part, right? Play around with this B. So namely, so to prove in this case, what we have to proof? 2 b Square is greater than b, to get a term b + 1 whole Square for b greater than or equal to 3. So let us open up this things, we get 2 b Square is strictly bigger than, opening up b + 1 whole Square, we get b Square + 2 b + 1 for b greater than 3. This is equivalent statement.

Now, I can, I therefore subtract b Square on both sides and we get b Square - 2 b - 1 is greater than 0 for b is greater than or equal to 3. Now, as soon as you get something of this form what is b Square - 2 b, you realize that this has the very favor of b - 1 whole Square. So, this can now be written as b - 1 whole Square - 2 because this was +, - 1 and (()) (17:30) +1 also here. So, this is -2, so b - 1 whole Square - 2 is strictly greater than 0 for b greater than 3.

Now, we already see that the expression b - 1 whole Square is coming out not by looking at A, but looking at what to prove (()) (17:52). And this particular expression actually not that hard to prove. Or in other words, we have proof that b - 1 whole Square is greater than 2 and this is obvious, namely b is greater than or equal to 3 then b - 1 is greater than or equal to 2 or in other words, b - 1 whole Square is greater than equal to 4 is strictly greater than 2, which is what we have proved.

So, actually speaking this proof and other proof are identically same except that one what with A and ended up with b. The other we simplified b first before we applied A implies B. So, these are the two proof techniques that we have.

(Refer Slide Time: (18:40)



Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a backward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.
- And if $C \iff B$ then $(A \implies B) \equiv (A \implies C)$.

So in other words, to finish up for proving A implies B, I just taught with an assumption B and step by step prove that B is true. Or we can do the backward proof, which basically means that which wants, which simplify B and then prove A implies B.

So you simplify B to C and then A implies B is same as to be A implies C. And since C has been simplified to C, A implies B would be an easiest thing to prove. So, this brings up to the end of this video lecture. We will continue our study on proof techniques particularly constructive proof in the next video lecture. Thank you.