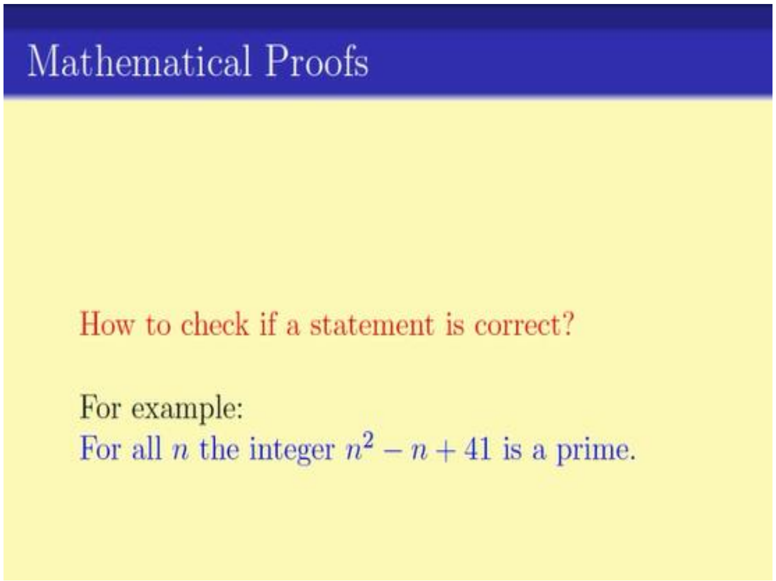
Discrete Mathematics
Prof. Sourav Chakraborthy
Department of Mathematics
Indian Institute of Technology – Madras

Lecture - 06
Formal Proofs

Welcome everybody to the second week in discrete mathematics. So, this is the sixth lecture, and we will be studying about short part of this course, which will be dedicated to mathematical proofs.

(Refer Slide Time: 00:21)



Mathematical Proofs

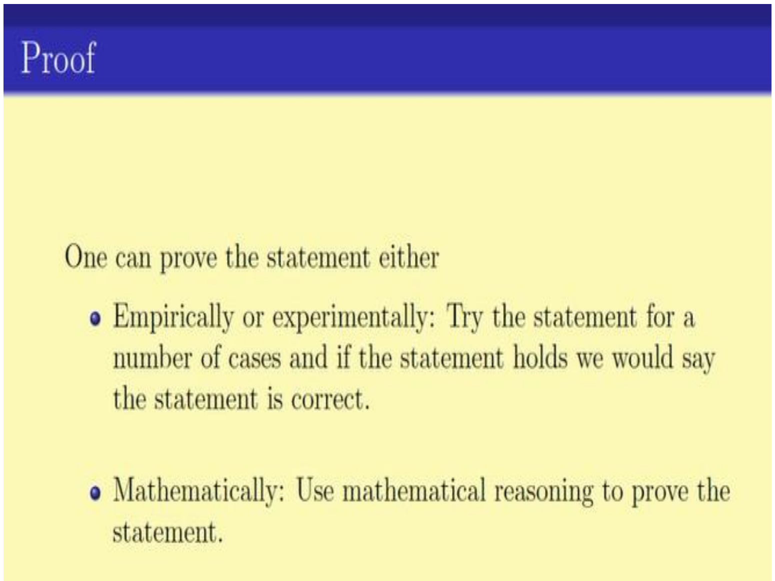
How to check if a statement is correct?

For example:
For all n the integer $n^2 - n + 41$ is a prime.

Now, what are mathematical proofs? In other words, if I give you a statement how do you check if a statement is correct? You must have faced this problem many times in your school or college or even in life. Now, there are two ways of going about proving this theory or proving a statement. For example, consider this following statement, for all n the integer n square – n + 41 is a prime, the prime number.

So, this is a statement I take. Now, if I ask you to check if this statement is correct, how will you go about it? So, there are two ways of checking if the statement is correct.

(Refer Slide Time: 01:26)



Proof

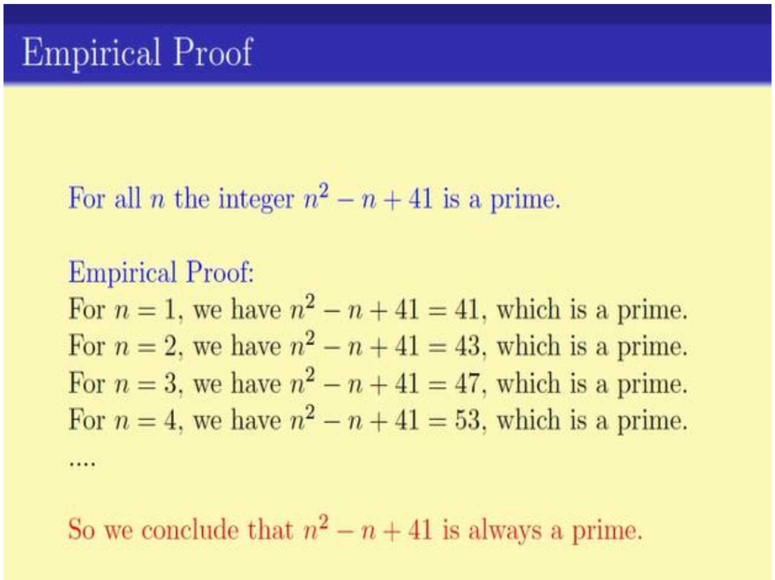
One can prove the statement either

- Empirically or experimentally: Try the statement for a number of cases and if the statement holds we would say the statement is correct.
- Mathematically: Use mathematical reasoning to prove the statement.

The first proof technique is partly called as empirical or experimental proof. That is, you would like to try this particular statement or any statement on a number of cases and if the statement holds for all the cases for which we have tried we would say, this statement is correct. So, this is one way of going about it. The second way is the mathematical way or in other words, use mathematical reasoning to prove the statement.

Here, we would like to go step by step and ensure that we have a full proof of that. Now, to start with let us look at experimental proof or empirical proof of that statement.

(Refer Slide Time: 02:27)



Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof:
For $n = 1$, we have $n^2 - n + 41 = 41$, which is a prime.
For $n = 2$, we have $n^2 - n + 41 = 43$, which is a prime.
For $n = 3$, we have $n^2 - n + 41 = 47$, which is a prime.
For $n = 4$, we have $n^2 - n + 41 = 53$, which is a prime.
....

So we conclude that $n^2 - n + 41$ is always a prime.

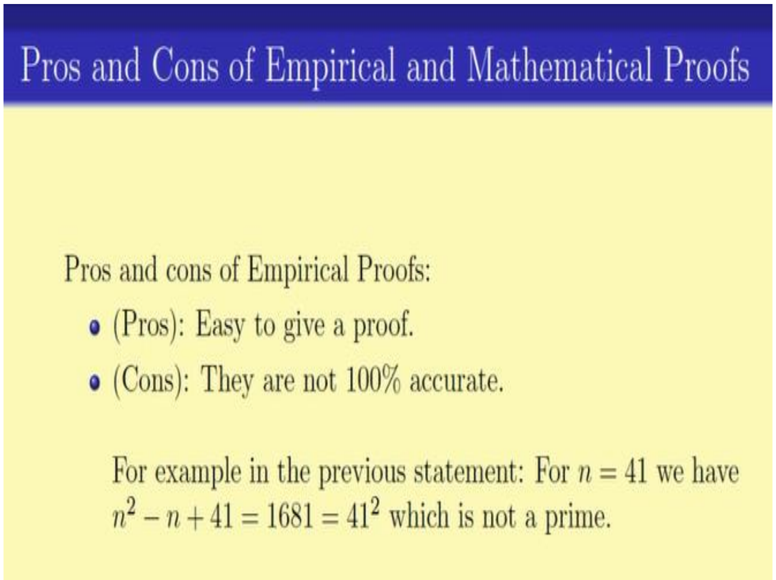
So, here in this statement for all n the integer n square – n + 41 is a prime. Now, how will you go about it? Of course, you want to check for various integers. For example, in empirical proof, say for n = 1, you get n square – n + 41 is 41, which is a prime. If n = 2, once again n square – n + 41 = 43, which is also a prime. For n = 3 you can check it that again, we get n square – n + 41 = 47, which is again a prime.

Again one more step. Again for n = 4, you can again check that the equation equals to 53, which is again a prime. And if you want to keep on checking for n equals to 5, 6, 7, 8, 9, and 10 and so on to 20, 30, 40 and you will see that this statement is correct. So, from this experimental proof, we can conclude that the number n square – n + 41 is always a prime, for all n, why? You have carried out some cases and those cases have revealed that it is a prime.

So, many times in our real life, we do make such kind of proofs, where we check if some statement is correct we sample or we test out these statements on a small number of points or instances and if for all of them we get the right solution or we prove this statement, we are happy and in that case, we say that this statement is right. But in mathematics that might not be the best way of going about.

So, for the case of empirical proofs, it has of course some advantages and some disadvantages. So let us see what are the advantages and disadvantages.

(Refer Slide Time: 05:03)



Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Empirical Proofs:

- (Pros): Easy to give a proof.
- (Cons): They are not 100% accurate.

  For example in the previous statement: For $n = 41$ we have $n^2 - n + 41 = 1681 = 41^2$ which is not a prime.

So, for the empirical proofs the first advantage is of course the fact that it is easy to give a proof. It is easy because we just have to check if the statement is correct or not for a finite number of instances. But, there is a downside to it. The downside is that they are not 100% accurate. Now it is obvious, why. Because (()) (05:36) earlier statement we have just tried out n, the statement n square – n + 41 is a prime, on just a finite number of points.

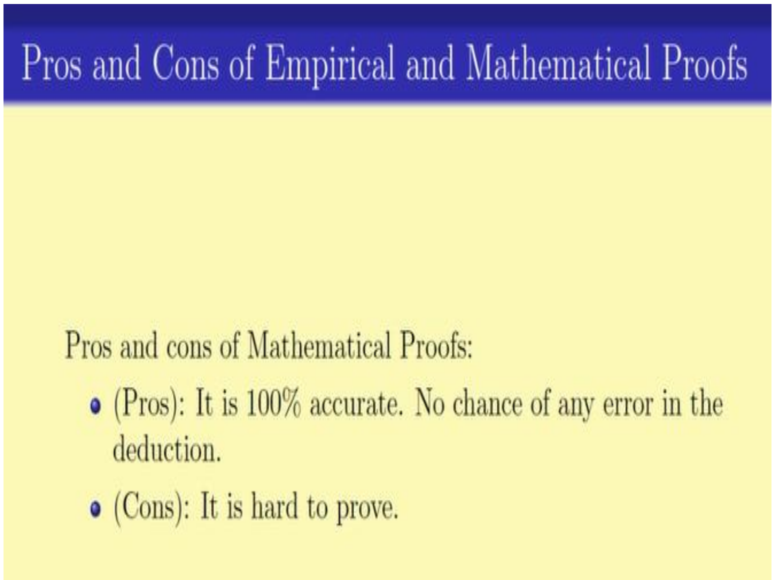
It is humanly impossible to test it out on infinite number of points. So, there might be a mistake somewhere. There might be some way for which it is not true and in fact that is what happens. For example, if you take n = 41 in that example, we do get n square – n + 41 is 1681, which is 41 square which is clearly not prime. I mean it is a square of an integer. So, why we had made some experiments and from most of the instances, we get this statement to be correct, yet this statement is not correct.

We don’t like this kind of proofs. Of course, if you are betting your money on something you would like to be 100% accurate and believe me, mathematic is something, where you bet your money. You are using your credit cards online. You are using your various bank statements so on and so forth. They are all online. All the security of all these internet transactions is based on some mathematical techniques or mathematical theory and unless they are 100% accurate you don’t want to risk your money on it.

So, if I say that your bank, your credit card is 100% safe I would like to say that your security of this whole system is based on a theory for which I have a mathematical proof. If I say that I have an empirical proof or an experimental proof, will you be satisfied with it? Because all you know is that for some particular instances, this whole security might break and you will lose all your money from your credit card or bank or whatever.

So, similarly say when you are going on a flight and I would like to say that ok, the security of the flight or the safety of the flight or the fact that these things bought is based on some mathematically proved statement. You don't want to risk your life on theorems for which we have an empirical proof. So, in other words we would like to have a mathematical proof all the time for every statement.

(Refer Slide Time: 08:54)



Pros and Cons of Empirical and Mathematical Proofs

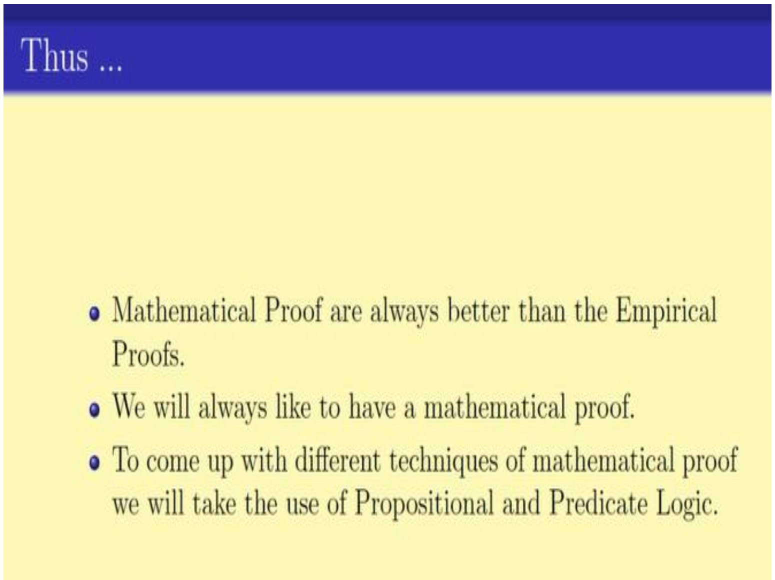
Pros and cons of Mathematical Proofs:

- (Pros): It is 100% accurate. No chance of any error in the deduction.
- (Cons): It is hard to prove.

The pros and cons of the mathematical proof is that, of course advantages are it is 100% accurate. There is no chance of any error in the deduction. So, it is safe completely. Everything is perfect. There is no chance that you have made a mistake. There is proof that all of this follows mathematical reasoning. The disadvantage is of course the fact that it is harder to prove. It isn't the easiest proof to come up with.

Why the empirical proof is easy because you just test it out in Tamil culture. Mathematical proofs can be extremely complicated. You might remember this thing from your high school or other pervious, where you have to come up with very creative ideas for getting a mathematical proof.

(Refer Slide Time: 09:55)



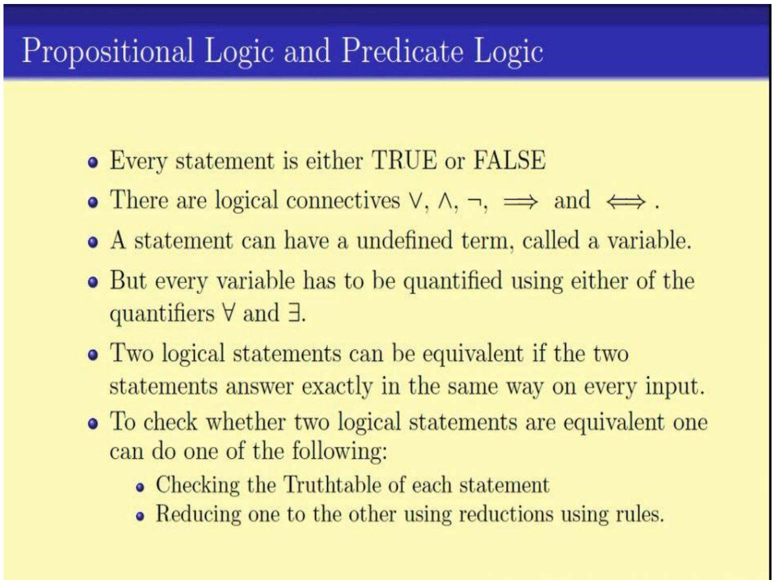
Thus ...

- Mathematical Proof are always better than the Empirical Proofs.
- We will always like to have a mathematical proof.
- To come up with different techniques of mathematical proof we will take the use of Propositional and Predicate Logic.

But all (()) (09:50) at the end of the day, mathematical proofs are always better than the empirical proofs because they give you 100% guarantee. And we would like to have mathematical proof all the time for everything. In this course, we will be dealing only mathematical proof and there will be no empirical and experimental proof at all. We will show you how to go around using a statement mathematically; with full logic, with full listening, so that it is 100% accumulate when you prove it.

No one can challenge it, no one can say that you have not, it is not full, it is not full proof. So to come up with different techniques of mathematical proofs, we will be using proportional and predicate logic, this thing that we have developed in the last week. So, you use this to understand different mathematical proofs, so that using them we can come up with solid proofs out.

(Refer Slide Time: 11:03)



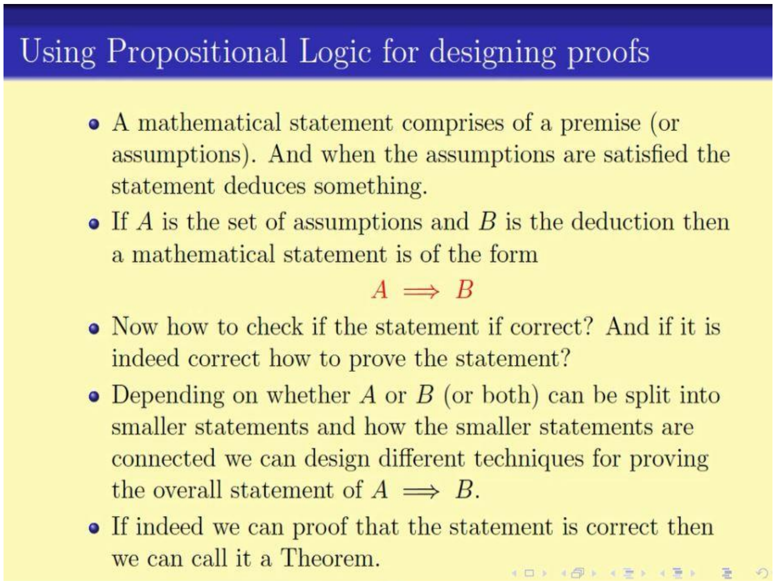
Propositional Logic and Predicate Logic

- Every statement is either TRUE or FALSE
- There are logical connectives $\vee$, $\wedge$, $\neg$, $\implies$ and $\iff$.
- A statement can have a undefined term, called a variable.
- But every variable has to be quantified using either of the quantifiers $\forall$ and $\exists$.
- Two logical statements can be equivalent if the two statements answer exactly in the same way on every input.
- To check whether two logical statements are equivalent one can do one of the following:
  - Checking the Truthtable of each statement
  - Reducing one to the other using reductions using rules.

So to recap what is proportional logic and predicate logic, proportional and predicate logic says that every statement is either true or false. There are connectives may be AND, OR, NOT, IMPLIED and IFF. A statement can have an undefined term, called a variable. But, every variable has to be quantified using either the quantifiers FOR ALL and THERE EXIST and here is the most important thing, propositional logic.

Two logical statements are said to be equivalent if the two statements' answers are exactly equal on every input. And this can be take either by using the truth table or by reducing one to the other by using some standard rules. I hope that you remember all these propositional logic and predicate logic that was done last week.

(Refer Slide Time: 12:30)



Using Propositional Logic for designing proofs

- A mathematical statement comprises of a premise (or assumptions). And when the assumptions are satisfied the statement deduces something.
- If A is the set of assumptions and B is the deduction then a mathematical statement is of the form

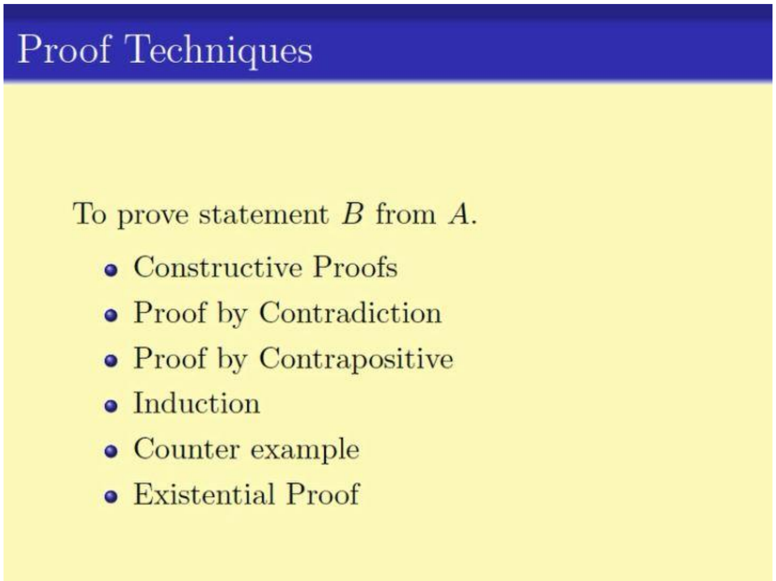
$$A \implies B$$

- Now how to check if the statement if correct? And if it is indeed correct how to prove the statement?
- Depending on whether A or B (or both) can be split into smaller statements and how the smaller statements are connected we can design different techniques for proving the overall statement of $A \implies B$.
- If indeed we can proof that the statement is correct then we can call it a Theorem.

So now using on, how do you use prepositional logic for designing proofs. Now as I told you earlier also a mathematical statement or any statement for that matter comprises of a premise and when the premise and assumption are satisfied, the statement deduces something. On the other words, it is of this form A implies B, where A is the set of assumptions and b is the detection of the mathematical statement.

Now, how to check if this statement is correct? That is how to check the statement A implies B is correct? And if it is indeed correct, how will you prove the following form for this statement A implies B? So, depending on whether A or B can be split up into smaller statements, you would like to break up the problem of A implies B into smaller problems and apply different kind of techniques to them. And if you can finally end up proving A implies B, it is only there you will say that this statement is the theorem.

(Refer Slide Time: 14:16)



Proof Techniques

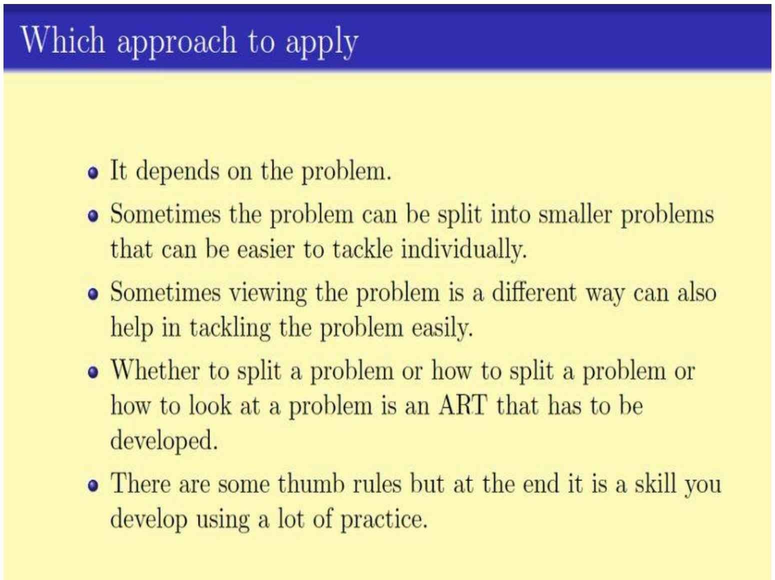
To prove statement B from A.

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

There are different proof techniques for (()) (14:21) this problem of A implies B, different mathematical proof techniques. I have listed out some of them - constructive proofs, proof by contradiction, proof by contrapositive, induction, counter example and Existential proof. We will go by one by one and see the different proof techniques. Again I repeat all of them are mathematical proof techniques and none of them are empirical or experimental proof techniques.

So, finally all of them will give you a 100% accumulate proof of as theorem. But, given a problem, the biggest question is which of the proof techniques to apply.

(Refer Slide Time: 15:15)



Which approach to apply

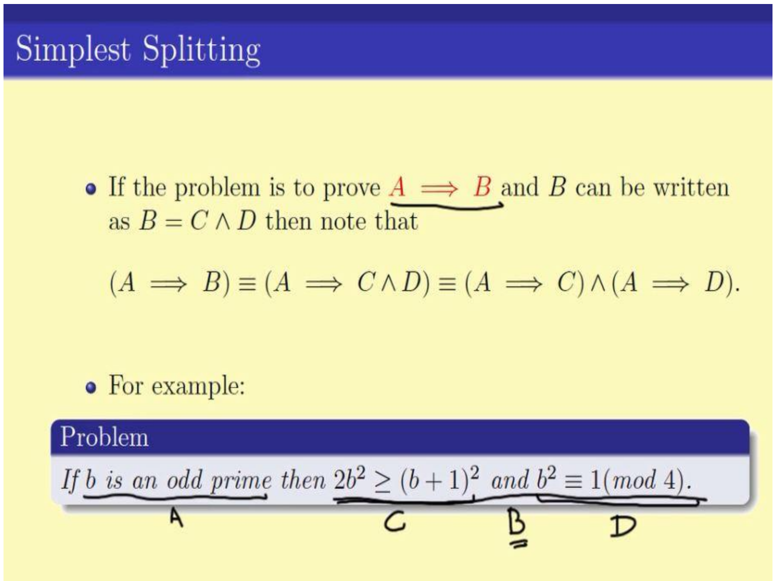
- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.
- Sometimes viewing the problem is a different way can also help in tackling the problem easily.
- Whether to split a problem or how to split a problem or how to look at 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.

So, even before I introduce the proof techniques let me tell you this step which approach to apply and I think is that it of course depends on the problem. Depending on the problem, you can decide it, have to decide which one will give you more suitable one to apply, which proof technique will make you like easiest. As I told you sometimes the problem can be split into smaller problems, each of which can be tackled easily, individually.

Sometimes viewing the problem in a different way can help you tackle the problem. Now whether to split a problem or how to split a problem or how to look at the problem is an art in itself and that is what has to be developed. In this course, we will be giving you all the tools that means all the techniques of attending the problem. We will be doing the number of problems as to understanding which approach will be the right approach to do.

We will give you some thumb rules but at the end of the day, it is you who has to have the creativity to understand how to a split problem, how to go about attending a problem. So although there are some rules at the end of the day, it is your skill that has to be developed with a lot of practice.

(Refer Slide Time: 17:04)



Simplest Splitting

- If the problem is to prove $\underline{A \implies B}$ 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

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

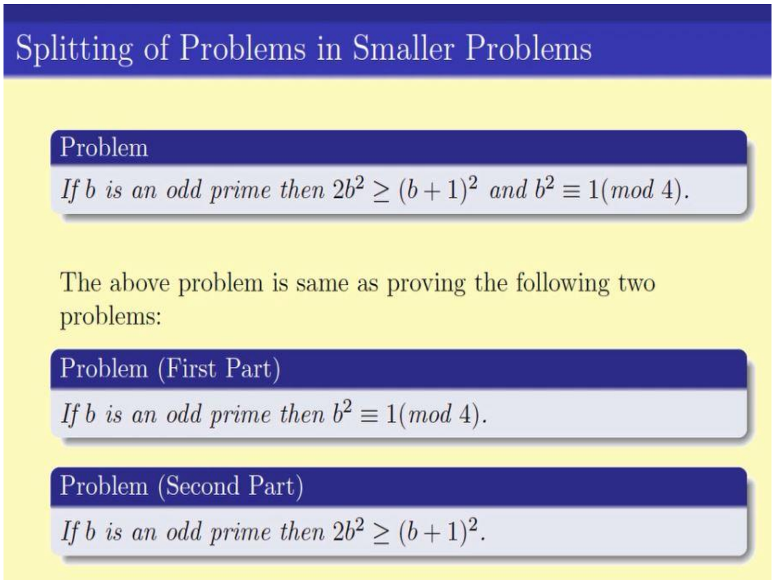
Now let us jump into the set of proof techniques. Now the simplest must splitting a problem is when you have A implies B and the B can be written as C AND D. The Propositional logic statement that kind of guides us this thing which says that if B can be split up into C and D, then A implies B, which is of course same as A implies C AND D is same as A implies C AND A implies D.

So in other words, if I give you this problem A implies B and you can split up B as C AND D that is good enough to first show me that A implies C and then showing me A implies D. Here in this example where we split the big problem into two smaller problems namely A implies C AND A implies D. For example, consider this problem if b is an odd prime, then 2 b square is bigger than or equal to b + 1 whole square and b square is congruent to 1 mod 4.

Here, I inform that you remember the notations of number theory that was introduced in the first week lectures. Now, if this is the problem to do, just try to understand, which is the B here, then the B is or if A as that A implies B. So, b the odd prime if this is A, then and we have this part, 2 b square is greater than b + 1 whole square and b square is congruent to 1 mod 4 is B.

Now, clearly here, the B can be split into two parts, namely this part and this part and that's what we will be doing. This will help us to follow, if this C and this is D, we can have A implies C AND A implies D.

(Refer Slide Time: 19:48)



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)

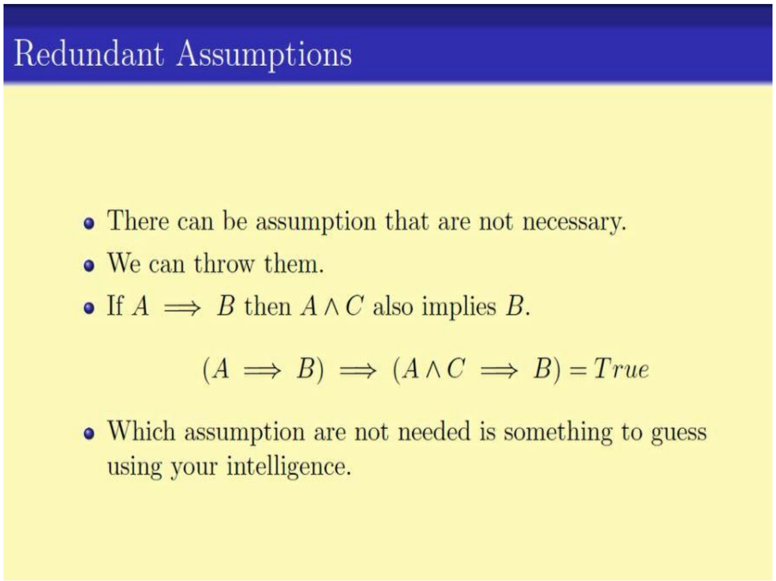
If b is an odd prime then $b^2 \equiv 1(mod\ 4)$.

Problem (Second Part)

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

Thus this problem can be split into two parts namely first part - if b is an odd prime then b square is congruent to 1 mod 4 and second part - if b is an odd prime then 2 b square is greater than or equal to b + 1 whole square. Here are the two parts that we got. So, a big problem that is split up into two smaller parts. Now so that one is that, we can handle each of the small problems individually. So, let us start with the first part. Let me - we can handle these small problems in this way.

(Refer Slide Time: 20:52)



Redundant Assumptions

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

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

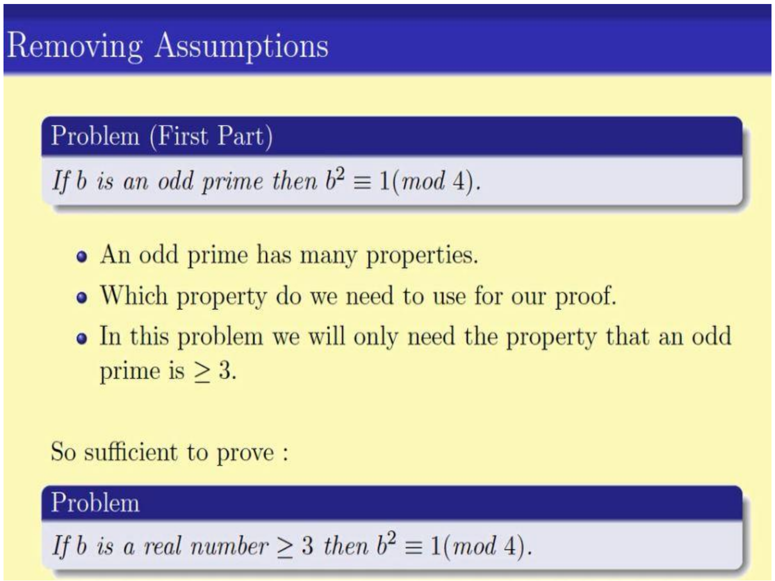
- Which assumption are not needed is something to guess using your intelligence.

Now before you move on to solving this two parts, let me tell you another thing namely sometimes the assumptions unbeaten that means some of the assumptions that has been told or not necessary. For example, so in that case we can throw them. If the assumptions are not necessary, we can just throw them. That means if A implies B then A AND C also implies B. This is the statement that we can prove that A implies B implies A AND C implies B is also true.

So, if A AND C is the given assumption but I am able to prove that A implies B that means this C was a redundant assumption and we can throw it. In that case, A AND C implies B, for this statement is good enough to prove this statement A implies B. Now throwing the redundant assumptions helps us to clean out the problem and get more focused in attending the problem. It helps us to understand, what is the important problem?

Although, it is not the easiest thing to understand before and quick assumptions are needed actively. Which assumptions are needed is something to guess using your own intelligence. This of course come with some practice and sometimes you can understand by time to solve this problem. You can understand which of the assumptions to be thrown out.

(Refer Slide Time: 22:50)



Removing Assumptions

Problem (First Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.
- In this problem we will only need the property that an odd prime is ≥ 3.

So sufficient to prove :

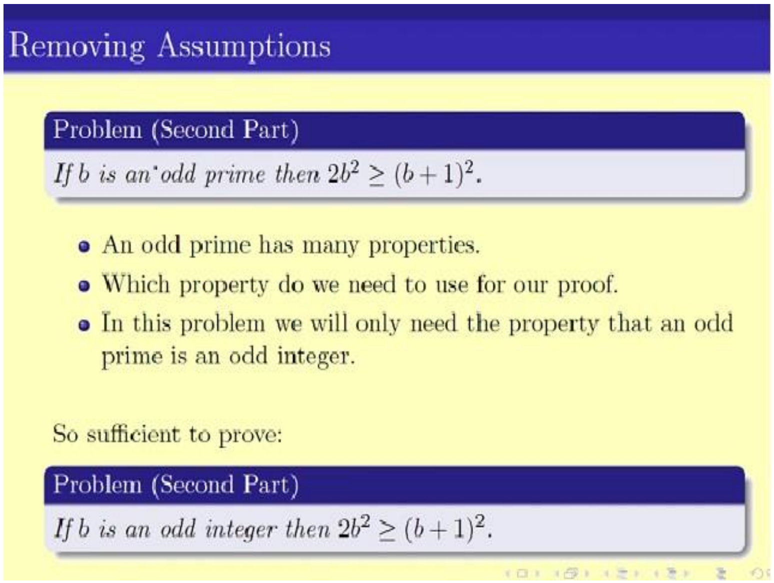
Problem

If b is a real number ≥ 3 then $b^2 \equiv 1(mod\ 4)$.

So what is that the realistic of problem which we have split in to two parts - first part and second part. Let us start with the first part, which says that if b is an odd prime then b square is congruent to 1 mod 4. Here, an odd prime has many properties. The question is that which property of the odd Prime do we need to use in this proof? Now, what is an odd Prime? A prime number which is odd. So, 2 is a prime but that is an even prime.

But, any other prime other than 2 is an odd Prime. So 3, 5,7,11,13,17,19 and so on are all odd primes. So, in this problem, it so happened that we will only need the property that an odd prime is bigger than or equal to 3. We don't need any other, we don't need a property of prime or other than the fact, it is bigger than or equal to 3. So thus, this first part is same as or is as good as proving or sufficient to prove that b, a real number greater than or equal to 3, then b square is congruent to 1 mod 4.

(Refer Slide Time: 24:40)



Removing Assumptions

Problem (Second Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.
- In this problem we will only need the property that an odd prime is an odd integer.

So sufficient to prove:

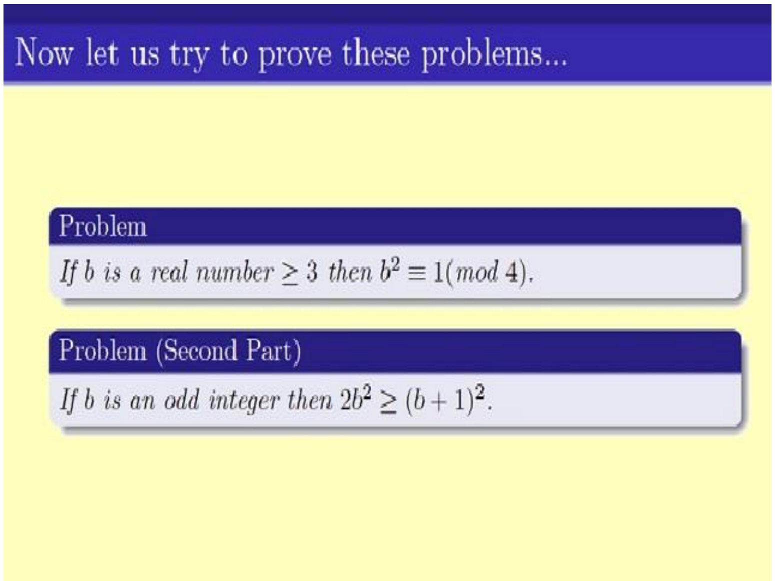
Problem (Second Part)

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

Similarly, let us go to the second part. It says that if b is an odd prime 2 b square is greater than or equal to b + 1 whole square. Now again, here b is an odd prime for which property of the odd prime to be used. And in this particular problem, all we need is b is an odd number or odd integer, that's what we need. So in this case, it is sufficient to prove that if b is an odd integer then 2 b square is greater than or equal to b + 1 whole square.

So, thus the main problem that we had has first we split up into smaller parts and then we showed that we can remove some of the assumptions and get two more precise statements, which will be hopeful easy to prove.

(Refer Slide Time: 25:49)



Now let us try to prove these problems...

Problem

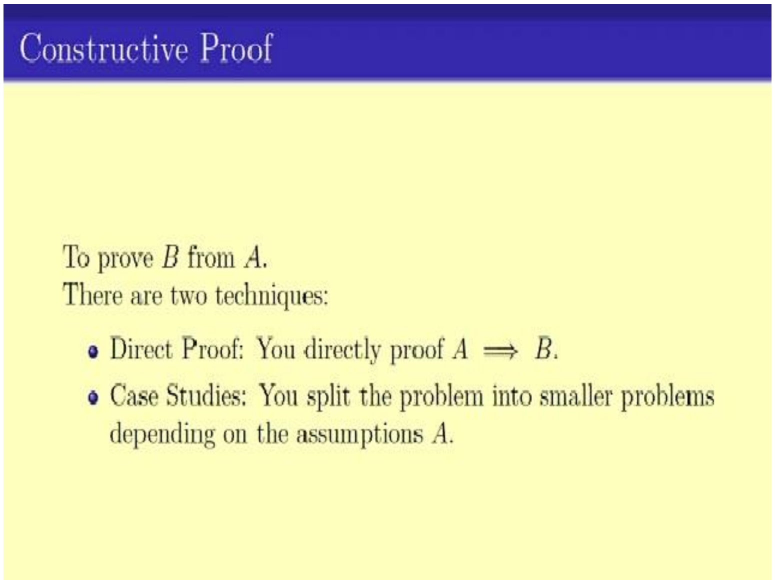
If b is a real number ≥ 3 *then* $b^2 \equiv 1 (mod\ 4)$.

Problem (Second Part)

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

So here are the two parts, problem first part - if b is a real number greater than or equal to 3 then, b square congruent to 1 mod 4 and second part - if b is an odd integer then, 2 b square is greater than or equal to b + 1 whole square. Now, how to go about to do the steps. So, we will give constructive proofs for these problems. Now, what we meant by the constructive proof?

(Refer Slide Time: 26:28)



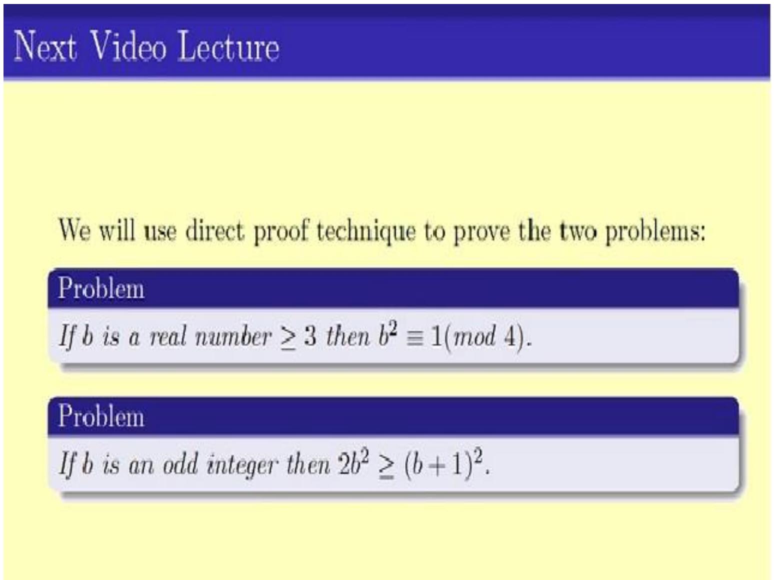
Constructive Proof

To prove B from A.
There are two techniques:

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

Constructive proof is something where to prove B from A, we use the idea of the two techniques. Namely, first we come to direct proof that will take A, we play around with it, we make some changes and we get B out of it, we call it direct proof. And second proof is that if you can split up the problem into even smaller statements depending on the assumptions of A.

(Refer Slide Time: 27:12)



Next Video Lecture

We will use direct proof technique to prove the two problems:

Problem

If b is a real number ≥ 3 *then* $b^2 \equiv 1(mod\ 4)$.

Problem

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

In the next video lecture, we will be solving the problems using the direct proof technique we will solve both the problems. This week we will be spending mostly on time on proof techniques using constructive proofs namely direct proofs and case study proofs. We will also be going a little bit into proof using contradiction, which is another way of a proof technique. Thank you.