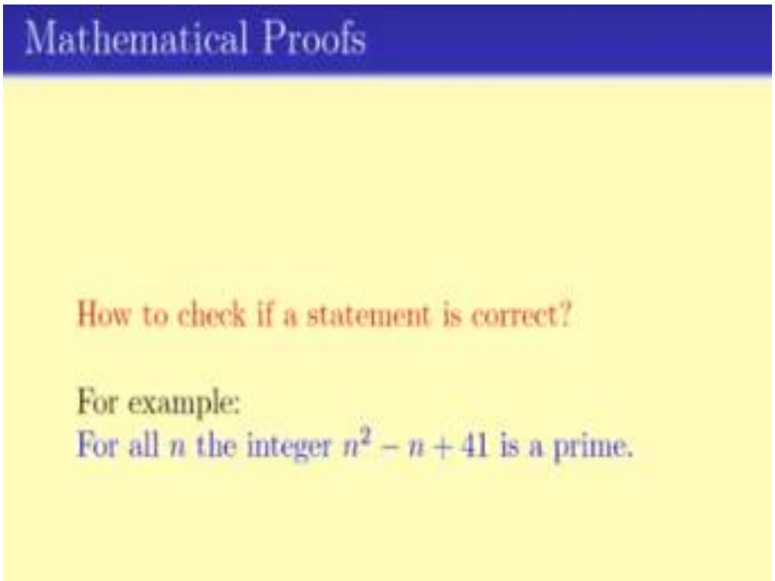
Discrete Mathematics
Prof. Sourav Chakraborty
Department of Mathematics
Indian Institute of Technology - Madras

Lecture - 48
Revising the Topics: Proof Techniques

Welcome back. So we are in the last few lectures in this discrete math course, so we will be using this time to revising what are all topics we have done or seen in this course. To start with, we have seen proof techniques.

(Refer Slide Time: 00:20)



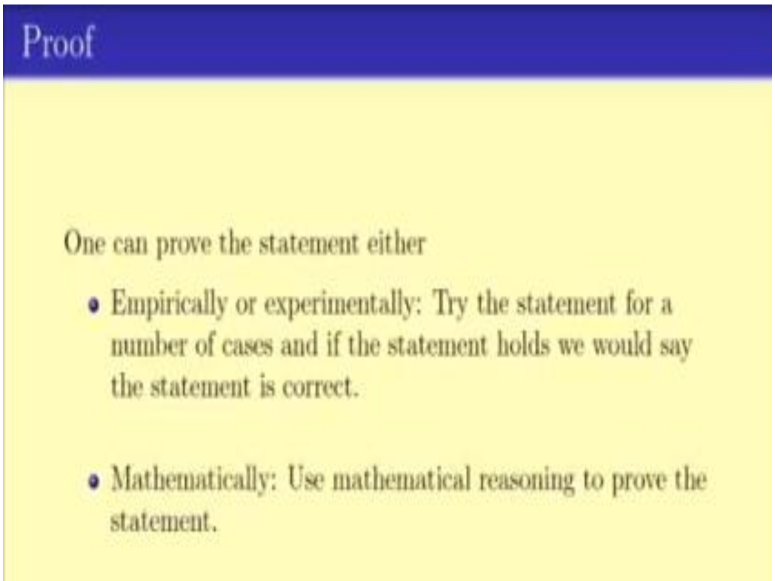
Mathematical Proofs

How to check if a statement is correct?

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

Now, this basic idea of proof techniques starts from the fact that we want to check whether a statement is correct or not. For example, say n square minus n plus 41 is a prime. Is this statement true or not? Now, there are two ways of solving this problem.

(Refer Slide Time: 00:43)



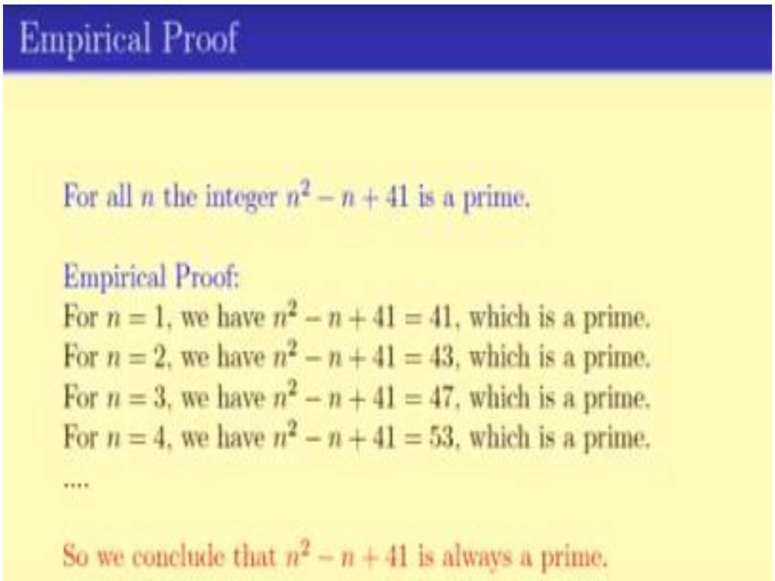
Proof

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 problem, first way is to prove it empirically or experimentally and second one is a mathematical proof where we use mathematical reasoning to prove this statement. Now, for an experimental proof, say, for these examples, the technique is to of course, try out for all different values of n and once we have convinced that for quite number of values of n, this statement is correct. We conclude that statement is correct for all n.

(Refer Slide Time: 01:25)



Empirical Proof

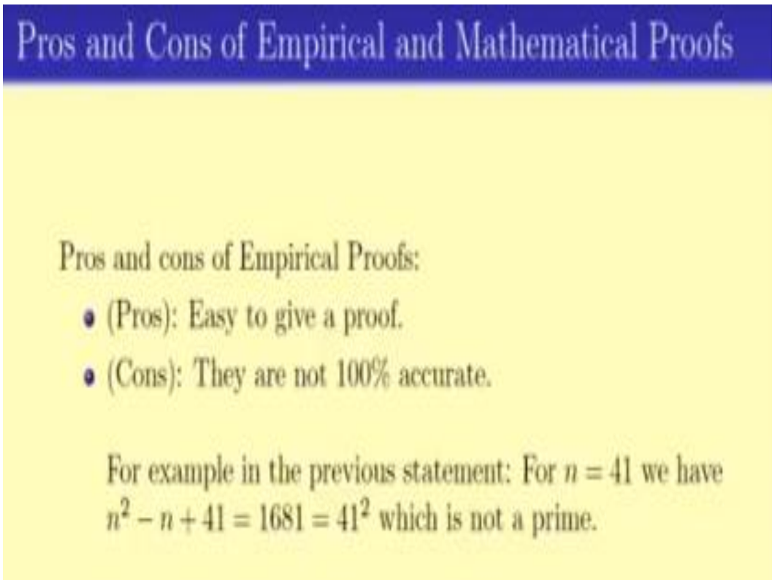
For all n the integer $n^2 - n + 41$ is a prime.

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.

The good thing of this empirical proofs of that, they are easy to prove but the back side of this is that, this proofs are not necessarily accurate 100 percent.

(Refer Slide Time: 01:46)



Pros and Cons of Empirical and Mathematical Proofs

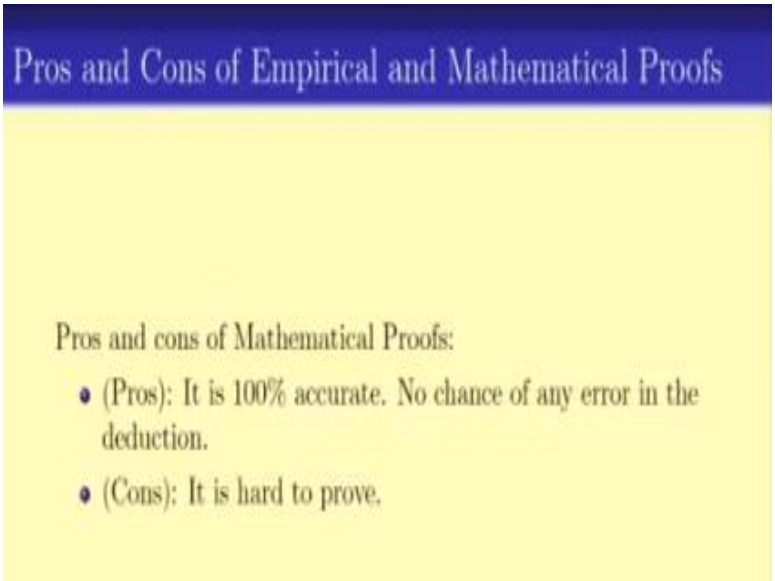
Pros and cons of Empirical Proofs:

- (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.

For example, in this case, why n square minus n plus 41 is prime for all small values of n. But for n equals to 41, it is not proved and if you have done it experimentally, we might have missed this n equals to 40. So the statement is false but empirically we might end up saying it is true.

(Refer Slide Time: 02:07)



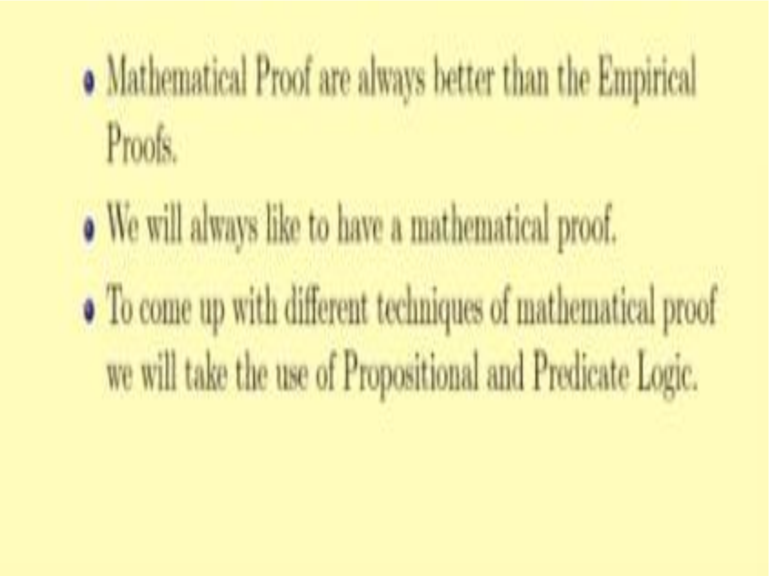
Pros and Cons of Empirical and Mathematical Proofs

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.

On the other hand, for the mathematical proofs, the advantage is there, it is 100 percent accurate and no chance of error in the deduction. But the reverse side is that it is hard to prove, it is not easiest simple proof.

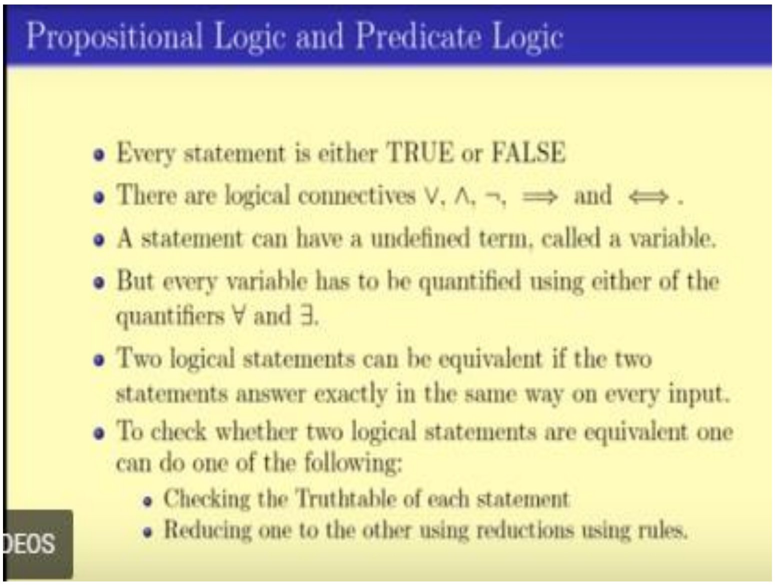
(Refer Slide Time: 02:28)



- 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.

Mathematical proofs are always better than empirical proofs because these 100 percent accurate if you can get it and we will always like to have a mathematical proof. Now to come up with different mathematical proof, we have to use this notion of propositional and predicate logic.

(Refer Slide Time: 02:50)

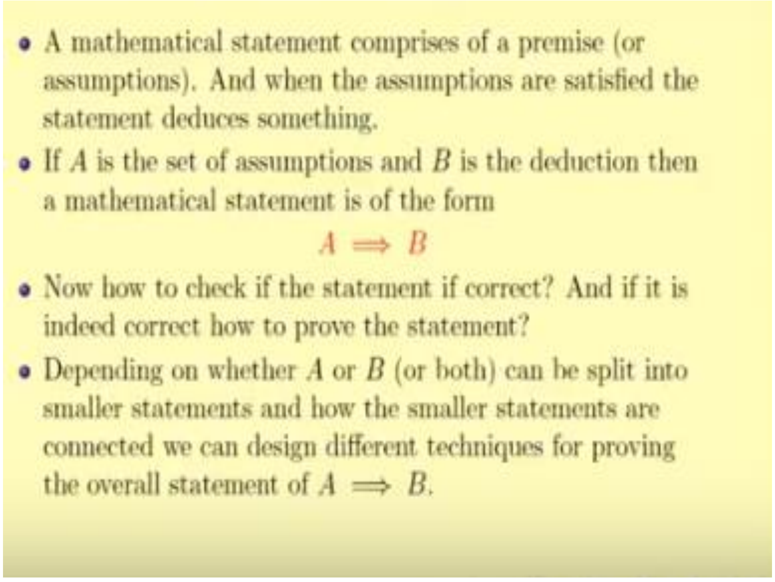


Propositional Logic and Predicate Logic

- 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.

And we have seen how to use a propositional and predicate logic, it basically is statements that are connected using AND, OR, NOT, IMPLIES, IFF and so on. And two quantifiers FOR ALL and THERE EXIST. There is various way of approaching the proofs and we have seen quite number of techniques.

(Refer Slide Time: 03:22)



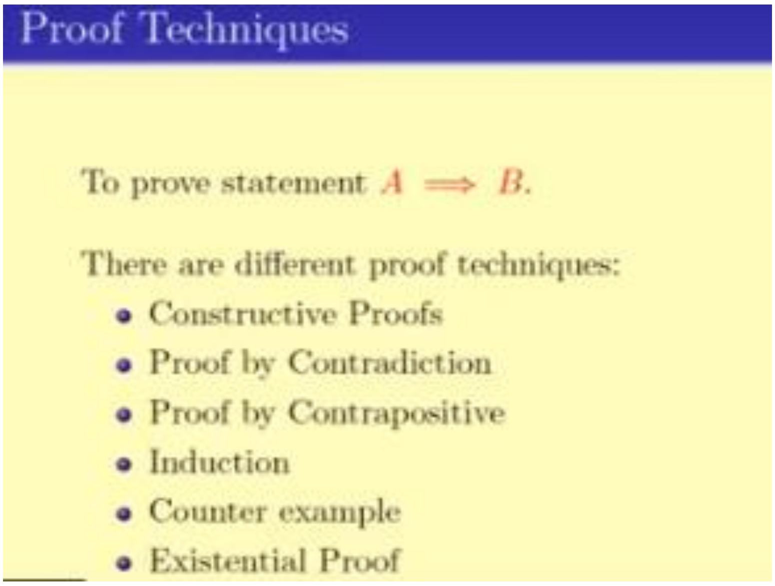
- A mathematical statement comprises of a premise (or assumptions). And when the assumptions are satisfied the statement deduces something.
- If A is the set of assumptions and B is the deduction then a mathematical statement is of the form

$$A \implies B$$

- 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 $A \implies B$.

So a statement always of the form A implies B. Now either there are various ways of proving with A implies B. Now depending on this structure of A as structure of B. For example, if A can be split into two AND of some numbers or B can be split into all of some numbers and so on and so forth. We might use some different proof techniques which are all of them are governed using this propositional logic statement.

(Refer Slide Time: 04:04)



Proof Techniques

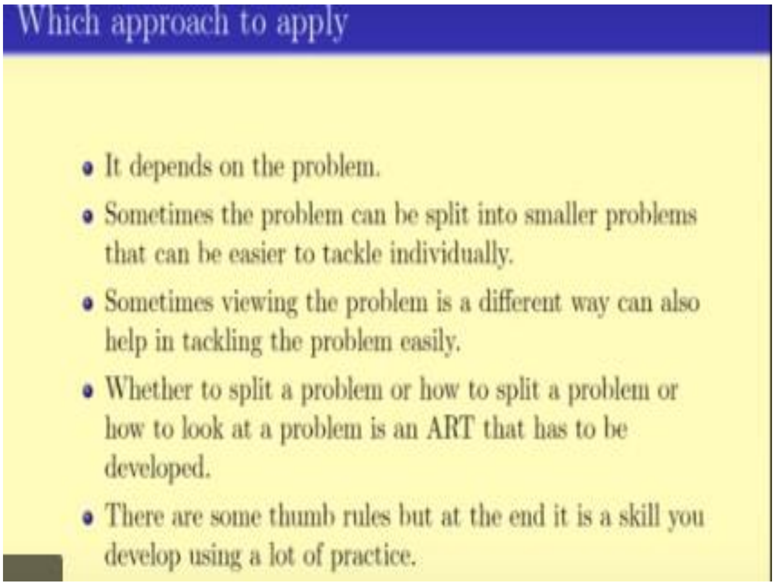
To prove statement $A \implies B$.

There are different proof techniques:

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

So, the proof technique that we have seen in this course are constructive proof, proof by contradiction, proof by contrapositive, induction, counter example. The existential proof, we have not seen in this course. But unfortunately, beyond the scope of this course to prove this existential proof or (()) (04:27) existential proof. But in case, you are interested, feel free to check in the internet what does existential proof means. It will require some amount of knowledge of probability to have solve these problems. To (()) (04:42) prove it using the existential proofs.

(Refer Slide Time: 04:52)



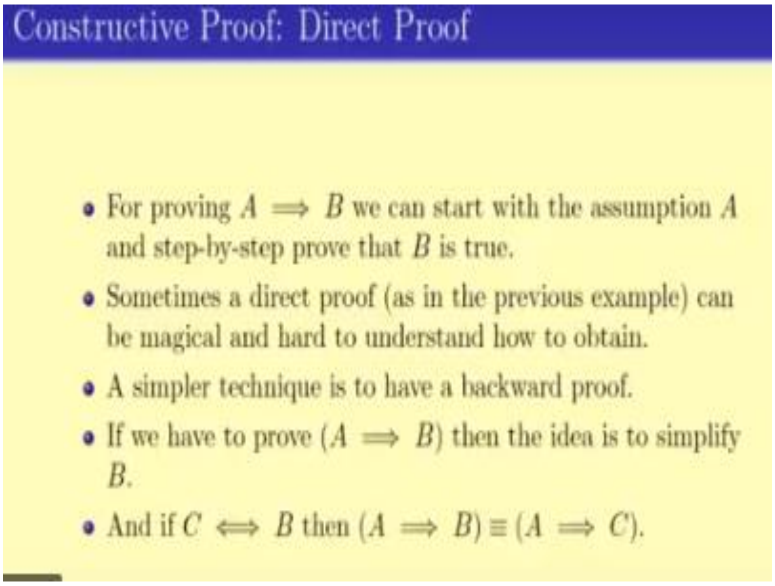
Which approach to apply

- 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.

Now the main questions is that, we had so many different proof technique that we have and the question is that which proofs techniques to apply and the basic idea is that there is no thumb rule for all any of these proof techniques. You have seen quite a lot of examples of has to for a which problem or which kind of problem, which kind of proofs can be helpful. So, there is some thumb rules that are there which can be used in practice.

But, there is no proper law that is has to be applied before. Hence, it is more often art that has to be developed. I am not going to go through these problems line by line and just going to revise them. Just for example, if B can be written as C and D, then we could split up into smaller problems. Similarly, they might be some redundant assumptions inside A can be removed and sometimes proving something stronger can actually be easier to prove.

(Refer Slide Time: 06:00)



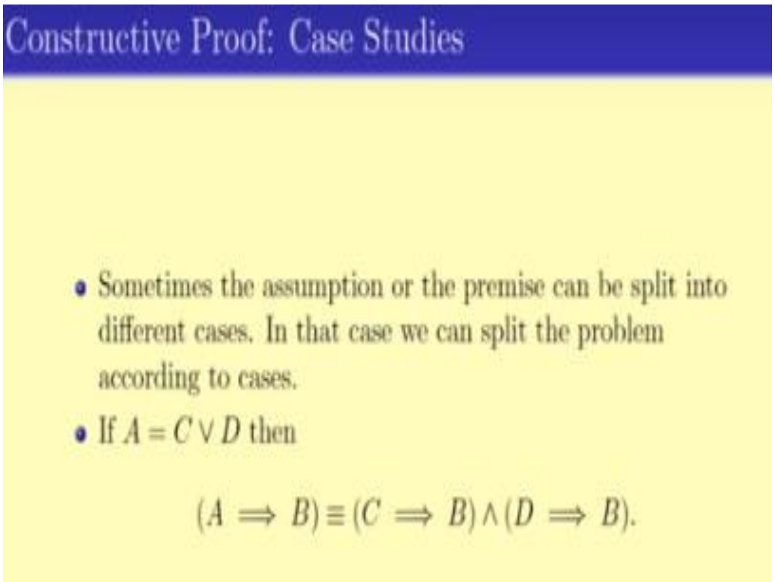
Constructive Proof: Direct Proof

- 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 $(A \implies B) \equiv (A \implies C)$.

After you have simplified this problem by using these various techniques - the just constructive proof technique has two cases. Number one is the direct proof where we starts from A and slowly end up solving B. Sometimes, the direct proof can be magical and hard to understand and a simpler proof technique might be to go from the backward. If we have to prove B then what is necessarily and what is necessary and so on.

Now, we saw that the direct proof techniques either from going for A to B or from B to A, both can be handy at times.

(Refer Slide Time: 06:56)



Constructive Proof: Case Studies

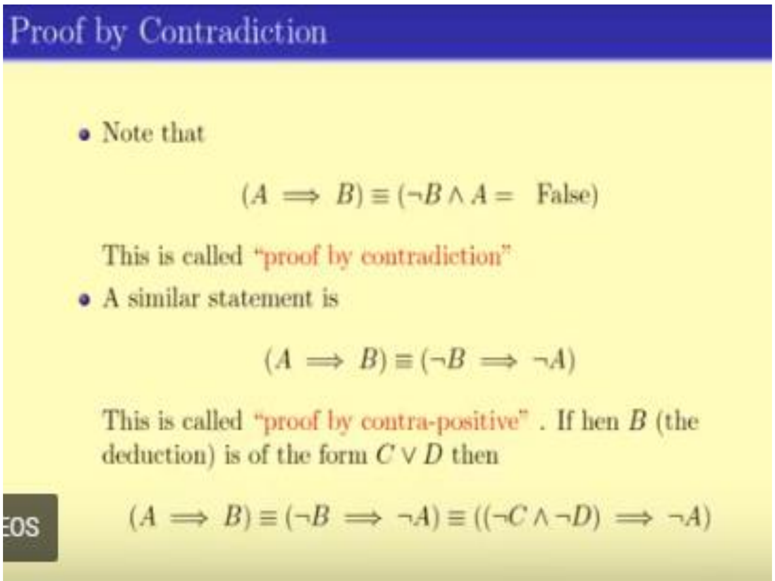
- Sometimes the assumption or the premise can be split into different cases. In that case we can split the problem according to cases.
- If $A = C \vee D$ then

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

Now, other than the direct proof, there is this another proof technique in the constructive proof which is the case study. The idea is that once you can break the assumptions, that with A implies B. In that case A into AND of smaller cases. Then you can split up into cases. We saw this one, variant pooling when we were at the certain kind of – number theoretic algorithms.

And case studies are extremely helpful for breaking down into cases then hence smaller number of problems.

(Refer Slide Time: 07:28)



Proof by Contradiction

- Note that

$$(A \implies B) \equiv (\neg B \wedge A = \text{ False})$$

This is called "proof by contradiction"

- A similar statement is

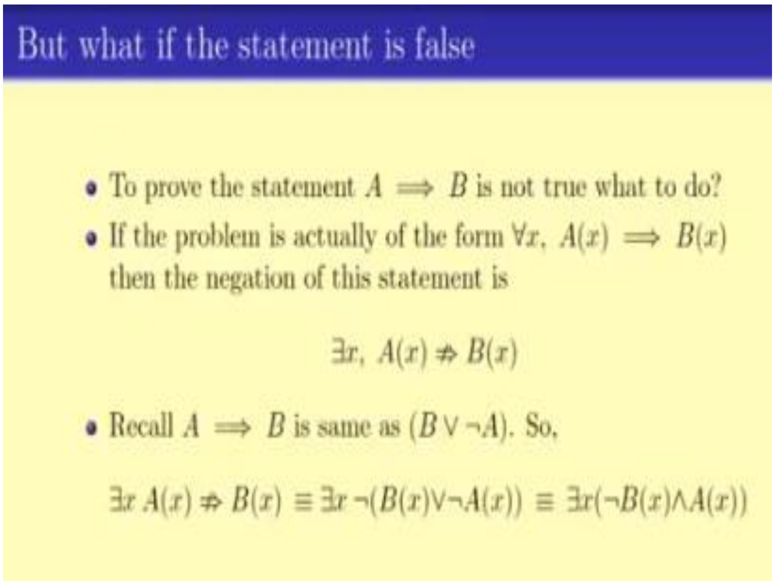
$$(A \implies B) \equiv (\neg B \implies \neg A)$$

This is called "proof by contra-positive" . If hen B (the deduction) is of the form $C \vee D$ then

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

Two other proof technique that was really helpful which were the proof by contradiction and proof by contrapositive. The idea is that to prove A implies B is same as assuming that B does not hold and A holds and then get to a contradiction, that is proof by contradiction or assuming, which mean that B does not hold prove that A does not hold, this is called proof by contrapositive.

(Refer Slide Time: 08:01)



But what if the statement is false

- To prove the statement $A \implies B$ is not true what to do?
- If the problem is actually of the form $\forall x,\ A(x) \implies B(x)$ then the negation of this statement is

$$\exists x,\ A(x) \not\Rightarrow B(x)$$

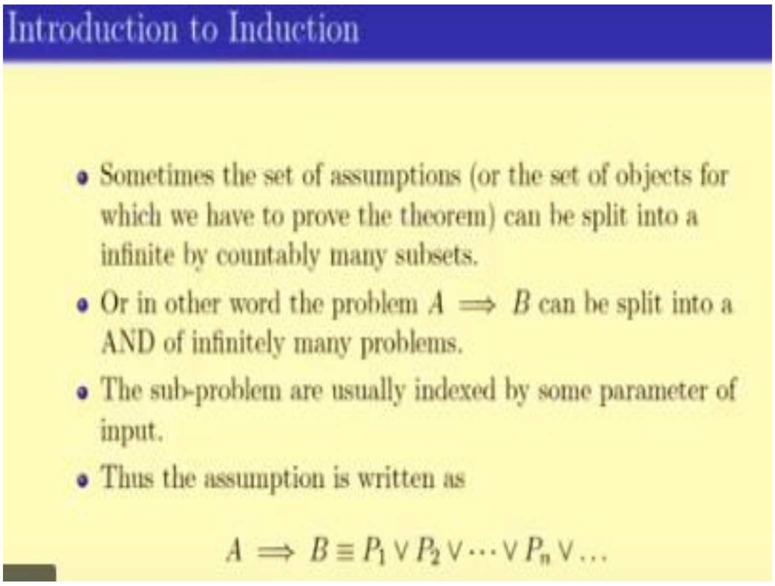
- Recall $A \implies B$ is same as $(B \vee \neg A)$. So,

$$\exists x\ A(x) \not\Rightarrow B(x) \equiv \exists x\ \neg(B(x) \vee \neg A(x)) \equiv \exists x(\neg B(x) \wedge A(x))$$

Now, if a statement is given which is not true then one way of solving it is to given example, where it is not true. For example, if the proof technique – the problem is FOR ALL A(x) IMPLIES B(x) then you want to prove the negation of this statement which is THERE EXISTS states A imply - not does not imply B(x) and which is same as giving an X. So this is what we call as counter example.

So we have direct proof, case studies, proof by contradiction, proof by contrapositive and counter example.

(Refer Slide Time: 08:56)



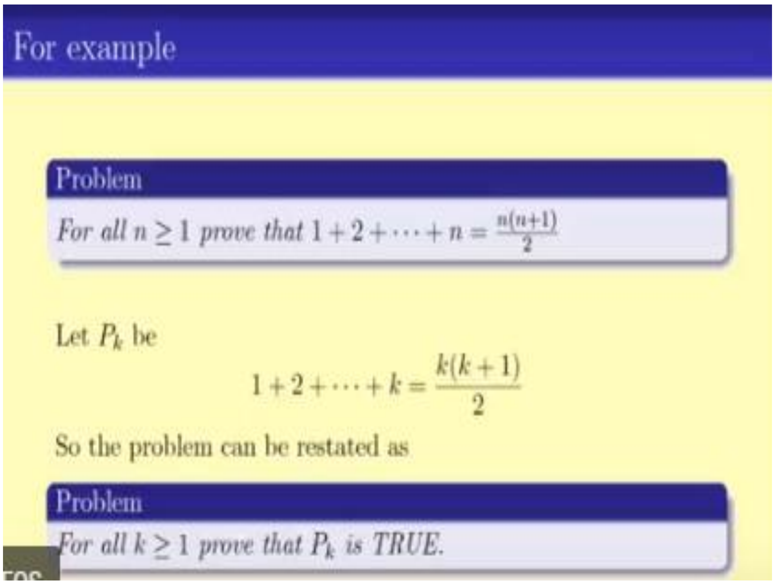
Introduction to Induction

- Sometimes the set of assumptions (or the set of objects for which we have to prove the theorem) can be split into a infinite by countably many subsets.
- Or in other word the problem $A \implies B$ can be split into a AND of infinitely many problems.
- The sub-problem are usually indexed by some parameter of input.
- Thus the assumption is written as

$$A \implies B \equiv P_1 \vee P_2 \vee \cdots \vee P_n \vee \ldots$$

Now, one more proof technique that we have spent quite a lot of time on is the induction. As I told earlier also it is the most powerful proof technique that you can imagine for the discrete math kind of subjects. The main idea is that if you can split the problem in doing infinitely many countably – infinitely but countably many subsets or problems, then you can solve them in a very clever way. For example, if you can split up A implies B of P1 to P infinity.

(Refer Slide Time: 09:38)



For example

Problem

For all $n \geq 1$ prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

Let P_k be

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

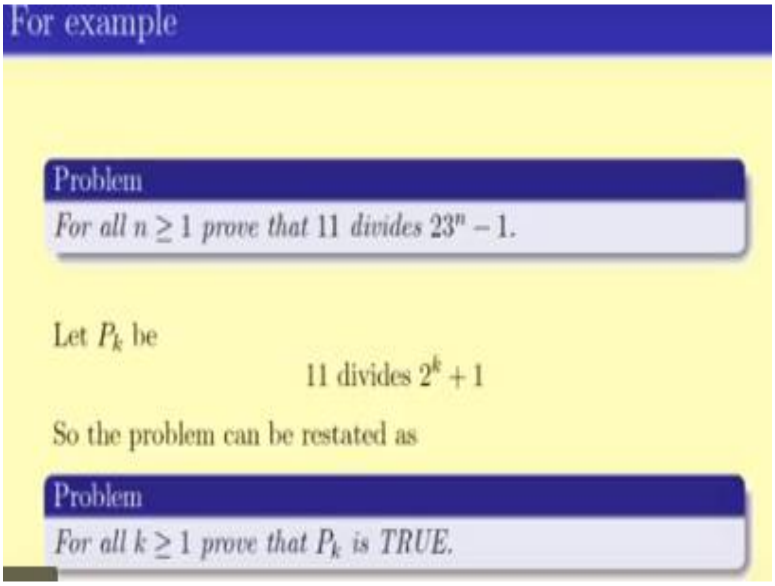
So the problem can be restated as

Problem

For all $k \geq 1$ prove that P_k is TRUE.

For example, in this problem, we have seen many of these kind of examples where to prove that the some of the first n numbers is n into n + 1 by 2. It is same as okay, for the some of the k numbers is k into k + 1 by 2. And the problem thus becomes for all A prove pk is true.

(Refer Slide Time: 09:59)



For example

Problem

For all $n \geq 1$ prove that 11 divides $23^n - 1$.

Let P_k be

$$11 \text{ divides } 2^k + 1$$

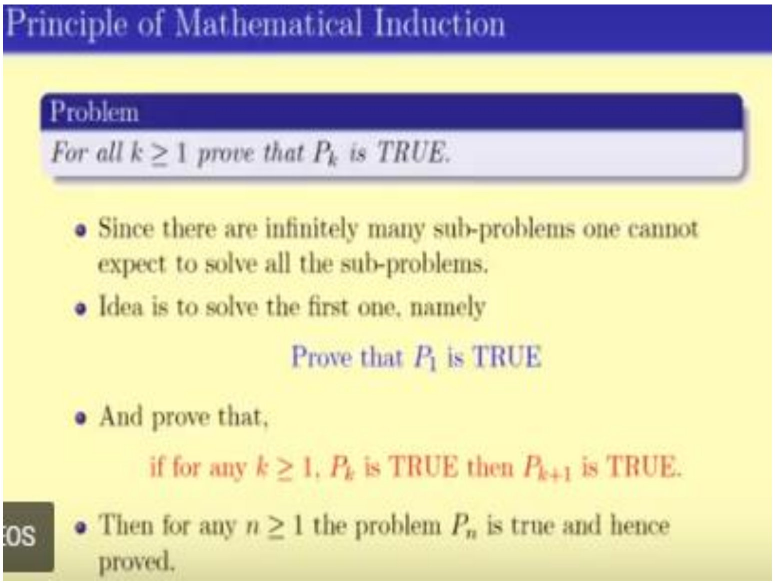
So the problem can be restated as

Problem

For all $k \geq 1$ prove that P_k is TRUE.

Similarly, for other problem that we have seen and once we split up this problem into smaller problems. The main idea is that so this is the problem, we have to solve for all k prove that pk is true. Then, infinitely many sub problems, so one cannot expect to solve all of them one by one.

(Refer Slide Time: 10:52)



Principle of Mathematical Induction

Problem

For all $k \geq 1$ prove that P_k is TRUE.

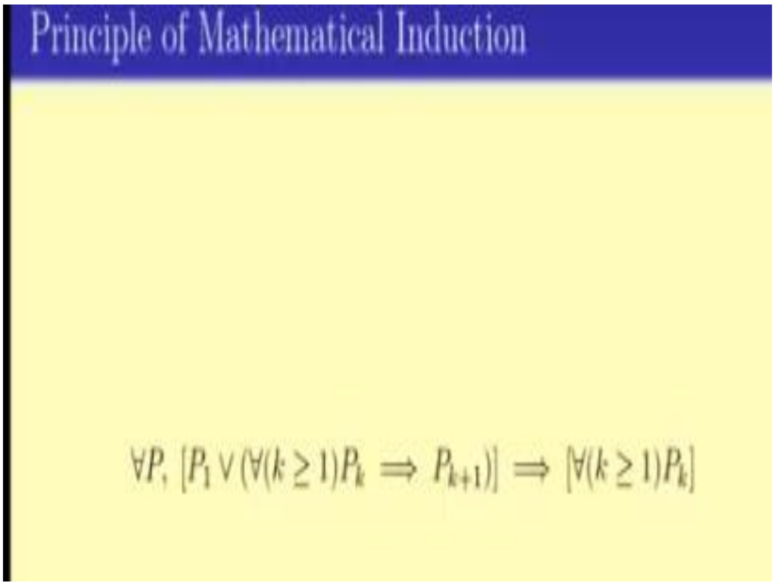
- Since there are infinitely many sub-problems one cannot expect to solve all the sub-problems.
- Idea is to solve the first one, namely

  Prove that P_1 is TRUE
- And prove that,

  if for any $k \geq 1$, P_k is TRUE then P_{k+1} is TRUE.
- Then for any $n \geq 1$ the problem P_n is true and hence proved.

But, the idea is first let us prove the first case p1 which is we called the base case. Then, if for all any k greater than 1, pk is true, then pk + 1 is true. And if you can solve it, then we would be done because p1 is true implies p2 is true. p2 is true implies p3 is true and so on and hence this would prove that for all nth value pn is true and hence the problem proved.

(Refer Slide Time: 11:04)

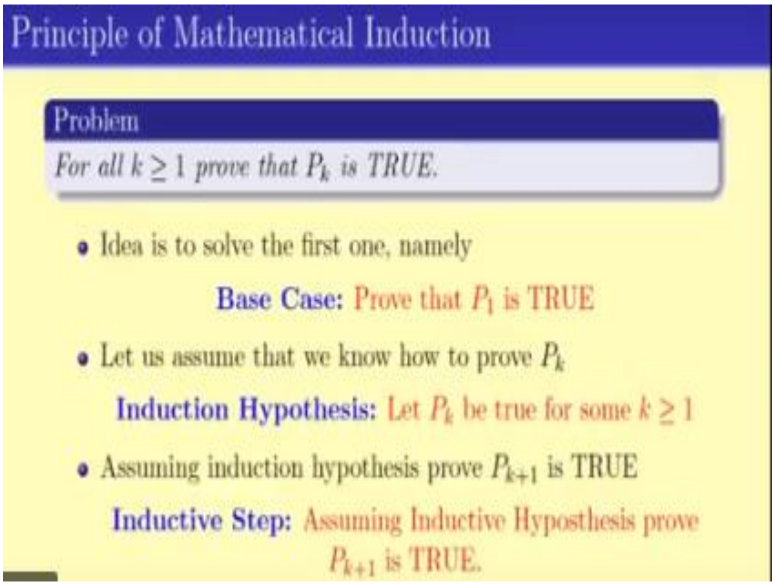


Principle of Mathematical Induction

$$\forall P, [P_1 \vee (\forall(k \geq 1)P_k \Rightarrow P_{k+1})] \Rightarrow [\forall(k \geq 1)P_k]$$

Now, this is true; Thanks to this principle of mathematical induction which tells us that this particular way of solving infinitely many problem is indeed true.

(Refer Slide Time: 11:14)



Principle of Mathematical Induction

Problem

For all $k \geq 1$ prove that P_k is TRUE.

- Idea is to solve the first one, namely

  Base Case: Prove that P_1 is TRUE

- Let us assume that we know how to prove P_k

  Induction Hypothesis: Let P_k be true for some $k \geq 1$

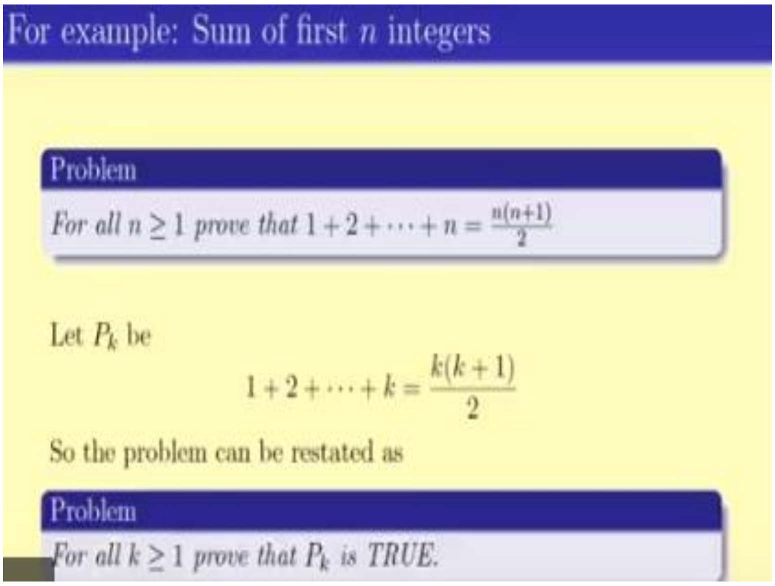
- Assuming induction hypothesis prove P_{k+1} is TRUE

  Inductive Step: Assuming Inductive Hyposthesis prove P_{k+1} is TRUE.

So, it sees at the base case, you have to induction hypothesis and you have the inductive state and if you can solve all the (()) (11:22) then we have done. As you have seen in the course, there are various different formulations of the induction hypothesis or the mathematical induction and depending on the problem again one might want to try out some kind of induction over the other.

But the point to note is that mathematical induction indeed teach –indeed an extremely strong proof technique and along with the other proof technique that we have, we have got our foundations solid for how to get mathematical proofs.

(Refer Slide Time: 12:05)



For example: Sum of first n integers

Problem

For all $n \geq 1$ prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

Let P_k be

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

So the problem can be restated as

Problem

For all $k \geq 1$ prove that P_k is TRUE.

And that is it. So in the next video, we will be revising our graph theory and linear programming modelling. Thank you.