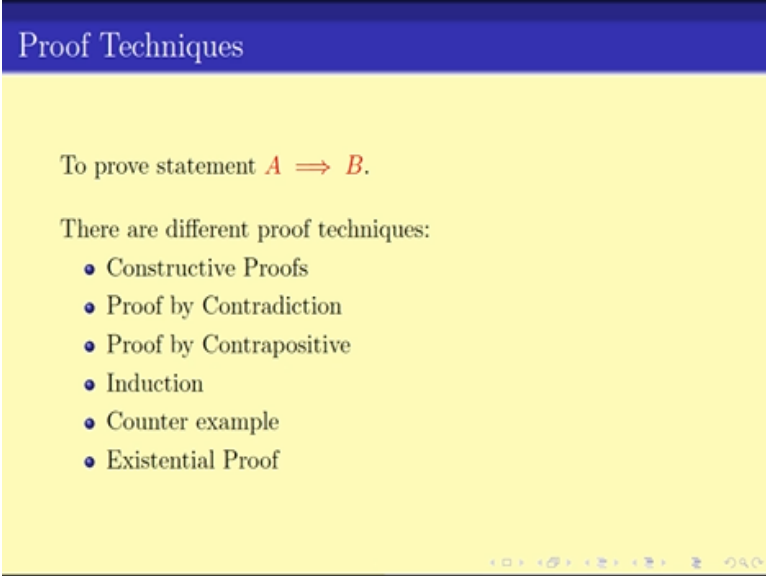


Discrete Mathematics
Prof. Sourav Chakraborty
Department of Mathematics
Indian Institute of Technology – Madras

Lecture - 09
Proof Technique Case Study (Part 2)

Welcome to the ninth video lecture in the discrete math. So this will be the fourth video lecture of this week and we will be concluding our study on the proof techniques using in particularly with proof technique study of constructive proof. In next lecture we will continue our study of proof techniques into proof by contradiction and other techniques. So to recap what we have done so far.

(Refer Slide Time: 00:48)



Proof Techniques

To prove statement $A \Rightarrow B$.

There are different proof techniques:

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

So we saw that to proof a statement like A implies B there can be various techniques that are there and we have seen that for some problems some of the techniques can be useful. One of the most important thing is to understand is which technique is to apply and we have discussed this thing earlier also that which technique to apply depends fully on the problem.

(Refer Slide Time: 01:10)

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 in 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.

Some problems can be split up into small smaller part or some problem can be viewed in a different way which might help in solving the problem but at the end of the day whether to split a problem or how to split a problem or how to look at a problem differently everything will depend on upon your creative mind. So in fact it will be giving lots of thumb rule for which one to apply when and so on.

But in the end your skill that you have to develop using lots of lots practice will be the only useful thing.

(Refer Slide Time: 02:17)

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

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

Now we started with understanding how to split a problem into two smaller parts if the deduction on namely to prove A implies B that part B can be split up into two separate things or in other words if B can be written as C and D then we saw that A implies B is same as proving A implies C and A implies D. Now we looked at this example and we saw that if the problem is something like if b is an odd prime then something and something.

(Refer Slide Time: 03:04)

The slide has a blue header with the title "Splitting of Problems in Smaller Problems". Below the header, on a yellow background, is a blue box labeled "Problem" containing the text: "If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 \pmod{4}$ ". Below this is the text: "The above problem is same as proving the following two problems:". This is followed by two more blue boxes. The first is labeled "Problem (First Part)" and contains: "If b is an odd prime then $b^2 \equiv 1 \pmod{4}$ ". The second is labeled "Problem (Second Part)" and contains: "If b is an odd prime then $2b^2 \geq (b+1)^2$ ". At the bottom right of the slide, there are small navigation icons.

And that can be split up into two parts namely, we can split up you can since there is 'and' in the beginning in the deduction so we can split up into two these parts. Part a and part one and part two or first part and second. So this was the first technique we learnt for time to solve a problem. Second one was the fact that to understand what properties of the assumption that are required.

(Refer Slide Time: 04:39)

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 .

$$(A \implies B) \implies (A \wedge C \implies B) = \text{True}$$

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

Namely there can be a lot of redundant assumptions and in there are redundant assumptions we would like to throw them away. Just to simplify the whole problem. The idea simple simply that if A implies B then adding some more assumptions for example A and C will also imply B. So in such cases one would like to just throw out with the C so in fact if we have to prove A and C implies B.

And we can prove A implies B then we would call this C as a redundant assumption and throwing it away would be useful for making this problem simple. Now again which assumption to be thrown or which assumption can be thrown will fully depend upon your intelligence. There are times when you will not able to understand which one to throw and which one not to throw. In that case you have to continue with various attempts.

(Refer Slide Time: 04:44)

Splitting of Problems in Smaller Problems

Problem

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

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

Problem (First Part)

If b is an odd prime then $b^2 \equiv 1 \pmod{4}$.

Problem (Second Part)

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

So for example in this problem that we saw after we split the main problem into two parts. in both of these parts part a and part first part and second part, the assumption was b is an odd prime and we saw that what properties of b required in either of these cases. So we what we saw is the first in the first part of what we need is that just the fact that b is an odd integer and the second one is that b then real number greater than or equal to three.

So that, so these are the two parts that are there. Now after i split this one the next technique that we apply was the proof, where the direct proof techniques so we use the direct proof to solve both the first and second part.

(Refer Slide Time: 05:36)

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.

So namely these are the constructive proofs. So a construction constructive proof has two parts. The direct proof namely A implies B, you work with A and you want to prove B or second part case study is when we split the problem into smaller problems.

(Refer Slide Time: 05:58)

Direct Proof: Example 1

Problem
If n is an odd integer then $n^2 \equiv 1 \pmod{4}$.

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

So the first part that was there or in other words if n is an odd integer then n square is congruent to 1 mod 4. This we did using direct proof technique. I am not going through the proof techniques fully. I am not going through the fool proof right now.

(Refer Slide Time: 06:21)

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 $2b^2 > b^2 + 2b + 1 = (b + 1)^2$.

We saw that in second example namely where we have to prove that if b then real number greater than or equal to three then $2b^2$ is greater than $b + 1$ whole square. And we saw that we can come up with the direct proof also but the direct proof did look a bit magical.

(Refer Slide Time: 06:51)

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

So the question was that sometimes the direct proof look a bit magical and hard to understand how to obtain that. So in such cases we discussed another approach namely a backward proof. The main idea is that if we have to proof A implies B , we start with the deduction that we have to get B and we (()) (07:17) we (()) (07:19) it or change it. And if we proof the C is identical to B so C is IFF B then proving A implies B is same as proving A implies C .

And since we have simplified B to C we would possibly be able to prove A implies C in a much simpler way.

(Refer Slide Time: 07:52)

Direct Proof: Example 2

Problem

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

Second Proof (Backward Proof):

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

$$\Leftrightarrow 2b^2 > b^2 + 2b + 1 \text{ for } b \geq 3$$

$$\Leftrightarrow b^2 - 2b - 1 > 0 \text{ for } b \geq 3$$

$$\Leftrightarrow (b-1)^2 - 2 > 0 \text{ for } b \geq 3$$

$$\Leftrightarrow (b-1)^2 > 2 \text{ for } b \geq 3$$

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

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

We saw the application of this particular technique when we solve this the second proof of this example. And we gave the backward proof so if we worked out, what started our proof from the in this this case at $2b^2$ is greater than $(b+1)^2$ and we worked our way through till what was referred to was simple enough that we could prove it directly.

(Refer Slide Time: 08:27)

Direct proof

- For proving $A \Rightarrow B$ 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 $(A \Rightarrow B)$ then the idea is to simplify B .
- And if $C \Leftrightarrow B$ then $(A \Rightarrow B) \equiv (A \Rightarrow C)$.

Okay so in other words for proving, for the direct proof or proving A implies B we can start with A and go step by step and prove B or we can also go do a backward proof in which case we kind of play with B simplified to C and then A implies B with same as proving A implies C . This is a very crucial technique that is applied along.

(Refer Slide Time: 09:10)

Sometimes proving something stronger is easier

If we have to prove $A \implies B$

- If $C \implies B$ then

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

- For example:

Problem

If b is a real number and $b \geq 2$ then $2b^3 > 3b + 2$

And there is one more technique that was there. namely sometimes we see that proving something harder can be actually be easier or in other word if we have to proof A implies B and if C implies B then if i can prove A implies C, then i would also be able to prove A implies B. So in other words we can prove something harder. So A implies C is clearly a harder thing to prove than A implies B but sometimes proving the harder thing can be easier.

So we solve the problem namely if b the real number and b is greater than equal two then $2b^3$ is strictly greater than $3b + 2$.

(Refer Slide Time: 09:55)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$. So,

$$2b^3 \geq 3b + 2 \text{ (for } b \geq 2)$$

$$\Leftrightarrow 2b^2 \geq 3b + 2 \text{ (for } b \geq 2)$$

$$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2 \text{ (for } b \geq 2)$$

$$\Leftrightarrow b^2 \geq 2b + 2 \text{ (for } b \geq 2) \text{ [Since } (b^2 - b) \geq 0]$$

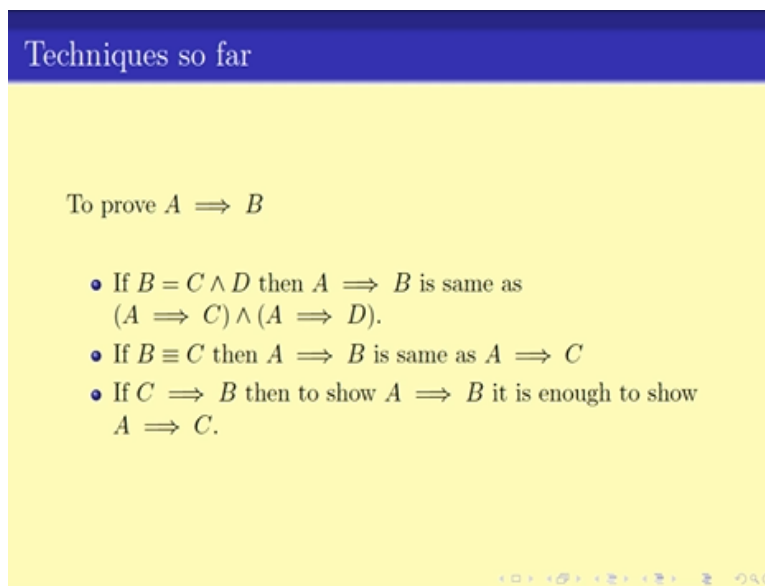
$$\Leftrightarrow (b - 1)^2 \geq 1 \text{ (for } b \geq 2)$$

And this is true as $(b \geq 2) \implies (b - 1) \geq 1$ and hence $(b - 1)^2 > 1$.

If this is the problem, we basically realize that there is a way of making it harder or in other words we saw that we kept on making this whole thing harder and harder we started. So for example here like the b^2 is greater than $2b + 2$ is a harder statement to prove than b^2 plus not harder than 2 but it is a stronger statement than this the earlier one which says that the $2b$ square is bigger than $3b + 2$.

But somehow by making this problem harder we are able to simplify the whole statement and that helps us to prove the main statement. This was one more technique that we have seen that can be applied for proving a problem.

(Refer Slide Time: 11:22)



Techniques so far

To prove $A \implies B$

- If $B = C \wedge D$ then $A \implies B$ is same as $(A \implies C) \wedge (A \implies D)$.
- If $B \equiv C$ then $A \implies B$ is same as $A \implies C$
- If $C \implies B$ then to show $A \implies B$ it is enough to show $A \implies C$.

The last of the technique that we have learned which we saw in last video was the proof by case study namely we talked about splitting the assumption into cases.

(Refer Slide Time: 11:28)

Splitting the assumption into cases

- 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

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

So sometimes the assumptions can be split with the assumptions in particular OR, AND like A is equal to C OR D, so the assumptions are 'OR' so A, C or D then A implies B is same as proving C implies B and D implies B. And this is the main thinking to do. The problem is that how to split the assumptions into parts or meaning how to write A equals C or D. Now this is not easy for some problems there is a kind of standard split, for some it's not.

(Refer Slide Time: 12:17)

Problem of last class

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Thus we have to prove that for any positive integer a

$$a^2 \not\equiv 2 \pmod{4}$$

So in the last class for example, we saw the example that if a and b are two positive integers then can we prove a square minus $4b$ cannot be equal to two in other words a square is not congruent to 2 mod 4. And in this particular case

(Refer Slide Time: 12:40)

Proof Technique: Case Analysis

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

If a positive integer a is divided by 4 then the possible remainders are 0, 1, 2 and 3.

We will solve in in case by case basis.

We split the problem into 4 case depending on the remainder when a is divided by 4 and show that for every case $a^2 - 4b$ cannot be equal to 2.

the main technique that we applied was that, we split the problem up based on whether the integer a as remainder 0, 1, 2 or 3 when divisible when divided by four. So it basically solved it in the in a case by case basis depending on the remainders. Okay so to let us take up a new problem in this video lecture and we will again solve this problem particular problem. So to start with

(Refer Slide Time: 13:22)

Prime Numbers

A positive number p is a prime is for all $1 < x < p$, x does not divide p .

A number that is not a prime is divisible by a prime.

If a, b are two integers such that p divides a but does not divide b then p does not divide $(a + b)$.

we start with prime numbers. We have defined prime numbers in your introductory week but just to just for people just to recap in refresh your minds here it is. So we say a prime number, p is the prime number if no other number less than p divides p okay. And this is an important thing if I have two numbers a and b if p divides a and p doesn't divide b then p does not divide a plus b .

This is something that we did in the first week and we will be needing particular number theoretic of derivation in this in this proof. So what is the problem?

(Refer Slide Time: 14:24)

Problem

Prove that the square of a prime number is always $1 \pmod{6}$, when the prime number is ≥ 5 .

Or in other words, if p is a prime number, such that $p \geq 5$, then $p^2 - 1$ is divisible by 6.

The problem is that prove that a square of a prime number is always $1 \pmod{6}$, when the prime is greater than or equal to five. So in other words if a prime, if the p is greater than equal to five then $p^2 - 1$ is divisible by six. Now here to start with let us understand what is the A ? So if A implies B right, so the A is p the prime number greater than or equal to five. That is the prime number; let us say what that the assumptions that are there.

And what is the thing that we have prove? To prove $p^2 - 1$ is divisible by six, so how can we split up the assumptions namely a p the prime number in two different cases.

(Refer Slide Time: 15:28)

Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 1 The remainder when p is divided by 6 is 0

Case 2 The remainder when p is divided by 6 is 1

Case 3 The remainder when p is divided by 6 is 2

Case 4 The remainder when p is divided by 6 is 3

Case 5 The remainder when p is divided by 6 is 4

Case 6 The remainder when p is divided by 6 is 5

Okay here we again using case by case basis. We split it by looking at the remainders, when divided by six. Now when a number is divided by six, what are the remainders that can remain? The remainder that can remain are of course 0, 1, 2, 3, 4 and 5. So I have this six cases depending on what remainders to use that will be left when you divide by six and these are the cases for which we will be solving the problem. So let us start with this first case.

(Refer Slide Time: 16:15)

Proof: Case 1

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 1 The remainder when p is divided by 6 is 0

Can a PRIME when divided by 6 have remainder 0?
That is can a prime p be $= 6k$ for some integer $k \geq 1$?

No. because $6k$ is divisible by 2.

Guess what the remainder is divisible by six, sorry remainder is zero. That means that the prime is divisible by six but can a prime be divisible by six? No. Of course not. If a prime divisible six that means the prime p is equal to $6k$ in which k it is of course divisible by two or divisible by

three right, so it cannot be a prime, by defining of a prime it cannot be divisible by any smaller number.

But here we can see that number which is six times some k integer k is of course divisible by two or three. So thus a prime cannot be of the order of cannot be six times k and hence the case one cannot exist okay. So case one does not exist, not a valid case. So done.

(Refer Slide Time: 17:25)

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 3 The remainder when p is divided by 6 is 2

Can a PRIME when divided by 6 have remainder 2?

That is can a prime p be $= 6k + 2$ for some integer $k \geq 1$?

No. because $6k + 2 = 2(3k + 1)$ and so is divisible by 2.

Similarly, let us go for this case three. So the case three again the remainder is two. In other words, p of the form $6k + 2$ and as you can see again since $6k + 2$ is divisible by two, it was two divide $6k + 2$, it leaves $3k + 1$ as the caution. And hence again this case cannot be a valid case. So if p the prime number then p cannot be cannot have a remainder two when divided by six.

(Refer Slide Time: 18:05)

Proof

If p ($p \geq 6$) is a prime then only 1 and 5 are the possible remainders possible when divided by 6.

Now, here i have left something for you okay. Note that just like we did the other two cases, i claim that the only two remainders that can be there when you divide by six are one and five. So 0, 2, 3, 4 are not possible remainders when divided by six. When divide by six only two remainders are one and five. I have proved that two of the cases cannot happen. You have to go home and prove that the other two cases does not happen.

(Refer Slide Time: 18:57)

Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 2 The remainder when p is divided by 6 is 1

Case 6 The remainder when p is divided by 6 is 5

So in other words we are left with two cases, namely case two which is that the remainder will be as a remainder one when divided by six and when the remainder four when divided by six, five, sorry remainder five when divided by six.

(Refer Slide Time: 19:20)

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 2 The remainder when p is divided by 6 is 1

$$p = 6k + 1.$$

$$\text{So } p^2 = (6k + 1)^2 = 36k^2 + 12k + 1 = 6(6k^2 + 2k) + 1$$

So $p^2 - 1$ is divisible by 6.

So now to prove these two cases one by one, so case one, so remainder one divided by six and p is the form of $6k + 1$, so p square if just square it up $6k + 1$ whole square which is comes down to some $36k^2 + 12k + 1$ which is 6 times $6k^2 + 2k + 1$. Now you might ask why do I split up like this, like divisible by six. Note that what is the problem we have to do.

The problem is that we have to prove that $p^2 - 1$ is divisible by six. We have a p^2 here, now we have a 1 here and we have something 6 times this. That is the main idea right. So $p^2 - 1$ is 6 times $6k^2 + 2k$ and this $6k^2 + 2k$ is a integer so $p^2 - 1$ is divisible by six and hence done. So this takes care of the case two.

(Refer Slide Time: 20:31)

Proof: Case 6

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 6 The remainder when p is divided by 6 is 5

$$p = 6k + 5.$$

$$\text{So } p^2 = (6k + 5)^2 = 36k^2 + 60k + 25 = 6(6k^2 + 10k + 4) + 1$$

So $p^2 - 1$ is divisible by 6.

Now for the case six, the last six case also has a similar thing this time the remainder is five. So p is the order of $6k + 5$, which means p square if you do the calculation everything is come to 6 times $6k$ square plus $10k$ plus 4 plus 1 . So we have 5 square left 25 which I can write it as 24 plus 1 and thus 6 times 4 plus 1 and hence again p square minus 1 is divisible by six.

(Refer Slide Time: 21:10)

Complete Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

We did a case by case analysis by considering the different remainders possible when we divide a number p by 6.

Some of the cases cannot happen because p is a prime.

For the other cases we did a case by case analysis.

Thus to prove the fact that if p the prime number, p square minus 1 is divisible by six, we divided into case by case various cases depending on what is the remainder when is divisible by six. Some of the cases cannot happen because p is a prime and we threw them away. We were left with two cases and for those two cases we did a case by case analysis. This was the this is one more example of a case study proof.

In the exercises that will be handed out on Tuesday or posted on Tuesday, there will be a number of more number of exercises for direct and proof in the case study. We will be solving some more of these problems in the video lecture where we will dedicated dedicate to problem solving.

(Refer Slide Time: 22:29)

Thus so far ...

To prove $A \implies B$

- Split the problem if $B = C \wedge D$
- Remove redundant assumptions.
- Sometimes its easier to proof a stronger statement
- Direct Proof
- Backward proof.
- Is $A = C \vee D$ then split into cases.

Thus so far what we have so far proofing A implies B we have seen a number of various techniques, here are some of the big ones. We split the problem if B is a written as C and D. We remove redundant assumptions. Sometimes it is easier to prove a stronger statement, we have the direct proof, we have backward proof and if A is C or D then we split it up into cases. Now okay let us move on. Let us start with a let us look at the following problem.

(Refer Slide Time: 23:10)

Infiniteness of Primes

Prove that primes are infinite.

That is, $\forall n \in \mathbb{Z}^+ \exists x > n$ x is a prime.

Now what are the primes that are there? The primes are said 2, 3, 5, 7, 11, 13 and so on right. Can you prove that the primes are infinite? That means there are infinite many number of primes. So there are many ways of asking the same quest. Can we say that given any big enough number there is a number which is a prime which is bigger than that number or is it that the number of prime is less than some fixed number, say is there only thousand number of prime or what?

Okay of course we have been asked to prove that primes are infinite. So how do you come up with a mathematical proof of taking that, there are not their infinite number of primes are not there or in fact there are infinite number of primes. Now for this proving this thing we will come up with a completely new proof technique.

(Refer Slide Time: 24:32)

Proof by Contradiction

- Note that

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

- To proof $A \implies B$

sometimes its easier to prove that

$$\neg B \wedge A = \text{False}.$$

This proof technique is what is called as proof by contradiction. So basic idea is that if we have been asked to prove A implies B, sometimes it is easier to prove not B and A is false. Now I would like you to go and check it for yourself this statements are, these two statements are indeed equivalent. I mean A implies B is equivalent to statement not B and A is false. So sometimes we will be using this thing and this is what is known as prove by contradiction.

Now what is the basic idea behind it?

(Refer Slide Time: 25:17)

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

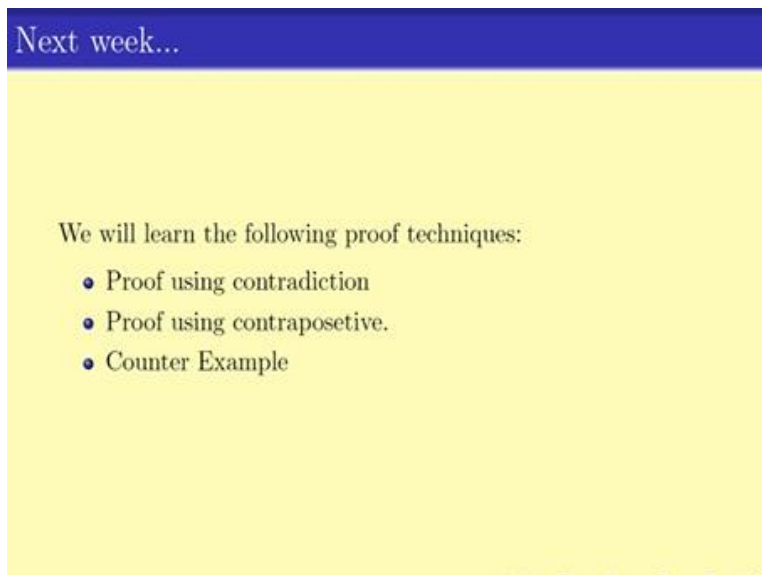
Attempt 2: Lets assume the earth is flat. Then when a ship came from the horizon the whole ship would appear at the same time.
But that does not happen - first the mast is seen then the whole ship. So a contradiction.

The basic idea is say consider this example that if I have to prove that the earth is flat. Now one way of proving it is that okay, you say that okay there is a ship coming from the horizon when a

ship coming from the horizon i first see the top of the ship and slowly the complete ship comes up. So you argue that the earth must be round and not flat. Then there is one more attempt of doing it, namely let us assume that the earth is not flat if the earth is flat then when the ship comes from the horizon before ship would appear in same time but that does not happen.

First the mast is seen or the top of the ship is seen and then the whole ship is seen. Thus say the contradiction. What you see or what happens is not same as what you thought would happen and the reason is that we have assumed something which is let us assume earth is flat and this assumption is wrong and hence we prove that earth is not flat. So this is the main way of attacking our proof by contradiction.

(Refer Slide Time: 26:59)



Next week...

We will learn the following proof techniques:

- Proof using contradiction
- Proof using contrapositive.
- Counter Example

We will of course come back next week and do a lot more problems on proof by contradiction then. So next week, we will be doing proof by contradiction; proof using contrapositive which is also similar to contradiction and counter example. Thank you.