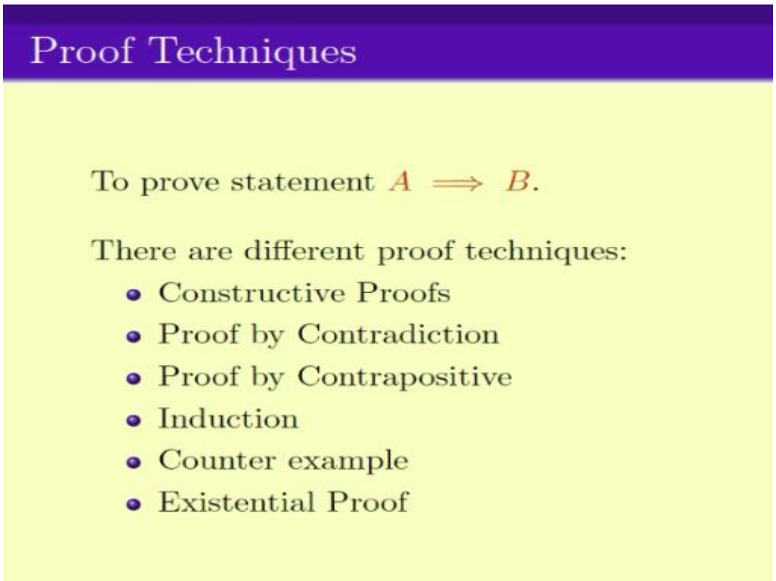
Discrete Mathematics
Prof. Sourav Chakraborty
Department of Mathematics
Indian Institute of Technology –Madras

Lecture - 10
Proof by Contradiction (Part 1)

Welcome everybody, to the third week of discrete mathematics. In this week, we will be continuing our study of proof techniques and in particular we will look at the proof technique of contradiction and contrapositive.

(Refer Slide Time: 00:22)



Proof Techniques

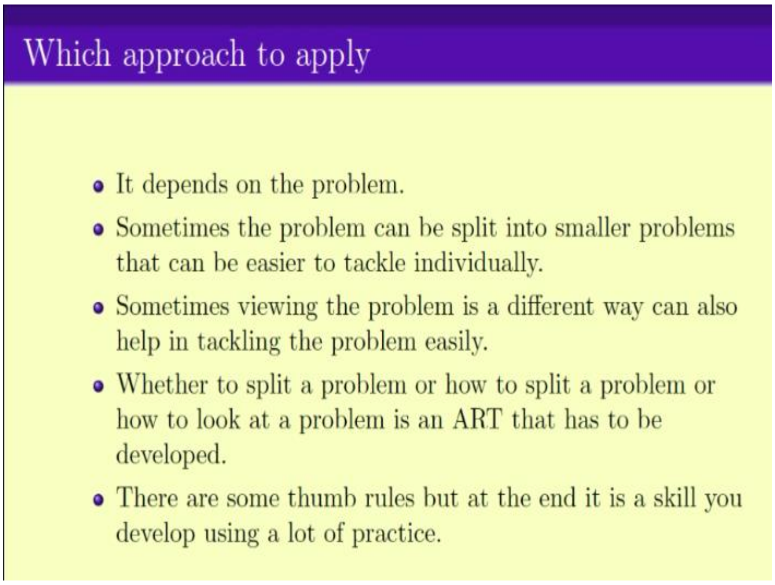
To prove statement $A \implies B$.

There are different proof techniques:

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

So to recall, we were dealing with the techniques of proofing a statement like A implies B. There are many proof techniques that can be applied for proving A implies B, can be constructive proof, proof of contradiction, contrapositive, induction, counter example, existential, etc. This is something I have told again and again in all the video lecture regarding proof techniques, that which proof to apply depends on the problem.

(Refer Slide Time: 01:00)



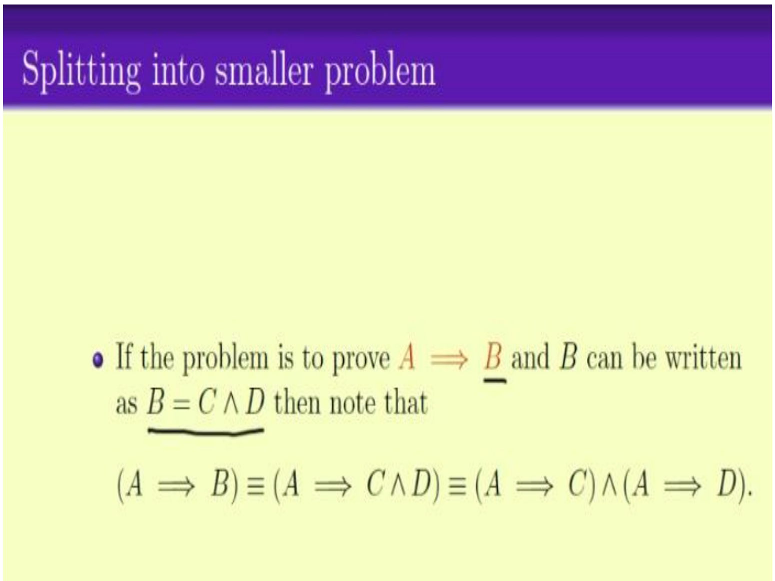
Which approach to apply

- 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.

In this course, we will be giving you all the different proof techniques by list, most of them. But, whether to, which proof technique to apply for which problem completely depends on you. Sometimes, the problem can be split into smaller problem, and that can make it easier. Sometime, viewing the problem in different way can make it easier. But, whether to split a problem or how to split a problem or how to look at in a different way, is an art that has to be developed by you.

In other words, there are some thumb rules that we will give, for example, if the problem is of this kind, then this kind of techniques can be helpful. But at the end of the day, which proof technique to apply depends fully on your skill. That you have to develop by doing a lot of practice.

(Refer Slide Time: 02:21)



Splitting into smaller problem

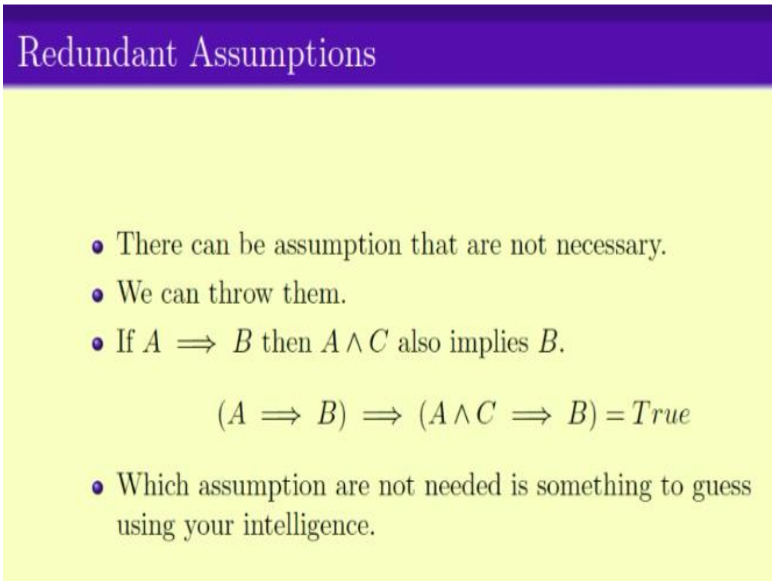
- If the problem is to prove $A \implies \underline{B}$ and B can be written as $\underline{B = C \wedge D}$ then note that

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

But till now, we are seeing some of the tricks. The first that we are to solve was, how to split a problem into smaller problems, when the B, that is the detection is of the form of C and D. So, in other word B in the form of C and D, then A implies B is same as proving A implies C and A implies D. We saw an example, how to use this particular way of splitting the problem, and help you to split a problem into two parts, you saw one such example.

The next technique that you learn was that sometimes reducing assumption can be helpful.

(Refer Slide Time: 03:06)



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.

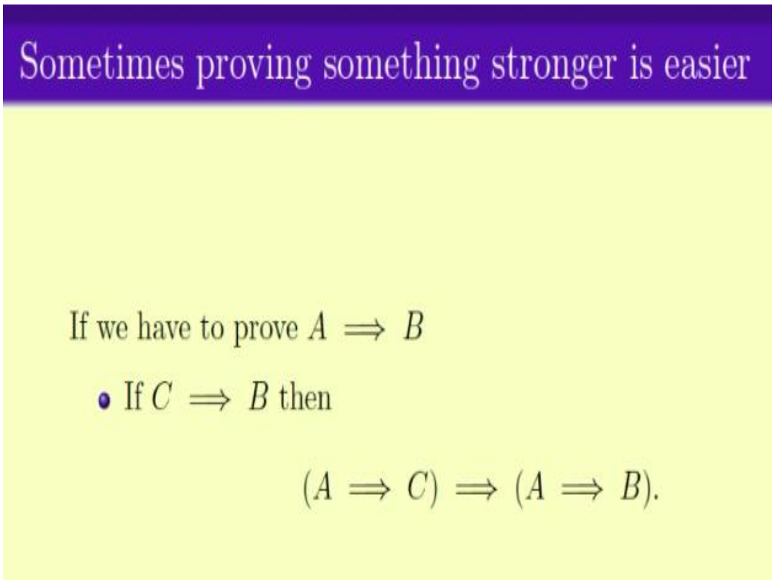
$$(A \implies B) \implies (A \wedge C \implies B) = True$$

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

In other words, there can be assumptions that are not necessary, and we can throw them away. For example, if I have been asked to prove A and C implies B all that I need is A, and I can prove A implies B, then that means that this C is a redundant assumption. And we can safely throw solve it away. But given the set of assumptions, one has to find out what are the actual subsided assumption that might be useful, the rest of them can be thrown away.

In other words, A implies B is good enough to make that implies A and C implies B. Again which assumptions are needed and which assumptions can be thrown away, depend on the problem and you have to identify them using your intelligence.

(Refer Slide Time: 04:31)



Sometimes proving something stronger is easier

If we have to prove $A \implies B$

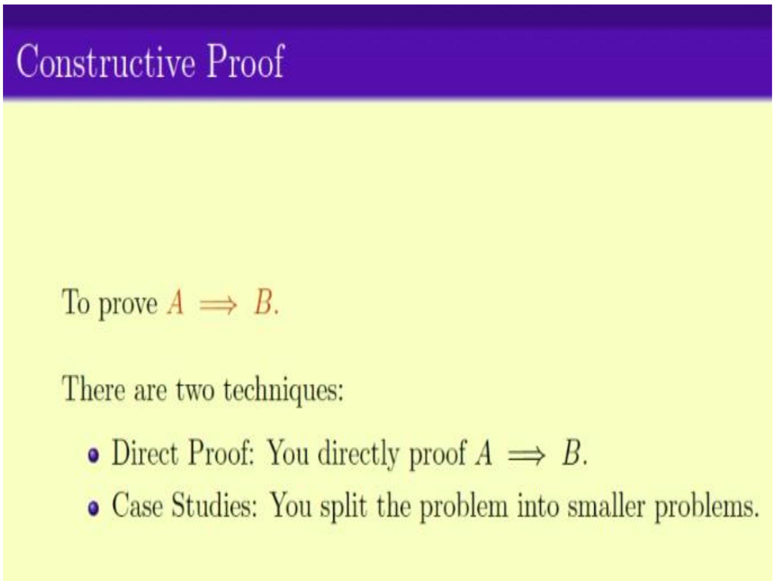
- If $C \implies B$ then

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

And third technique or third thing that we learnt was that, sometimes proving something harder can actually be easier. So in other word, if you have to prove A implies B and if we can prove that C implies B, then A implies B it follows. So in other words, why it might be harder to prove A implies C, but if we can prove A implies C, then we get A implies B. Sometimes, this harder problem technique is easier to prove.

For example, here note that A implies C is strictly harder than A implies B, but proving the harder statement can actually more helpful, more easier than following the easiest technique A implies B. On moving on, after the set of useful tricks we looked at the problem, and the first major approach of solving a problem namely constructive proof.

(Refer Slide Time: 05:48)



Constructive Proof

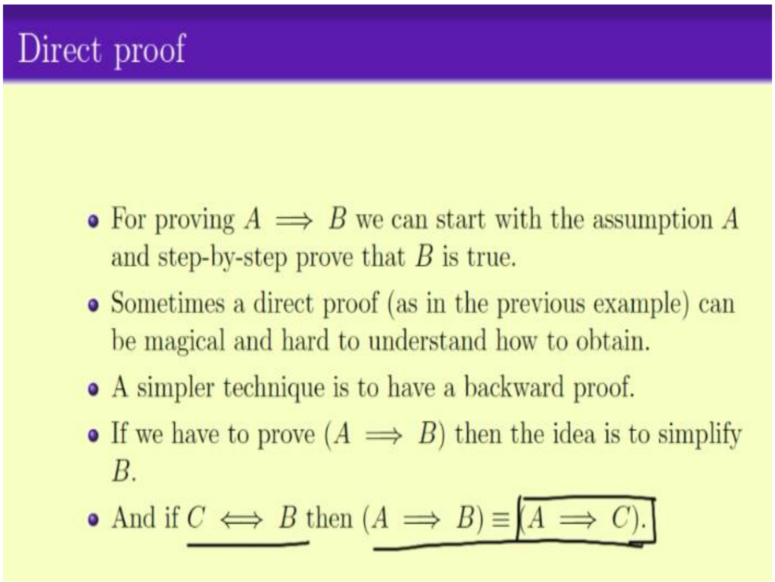
To prove $A \implies B.$

There are two techniques:

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

The idea of constructive proof is that if we have to solve A implies B you work with A and start working at it and end up with B. On split up the constructive proof into two parts, first part was the direct proof, we directly prove A, and we directly prove B from A. The second one was the case study, where you split the problems into smaller problems depending on A.

(Refer Slide Time: 06:30)



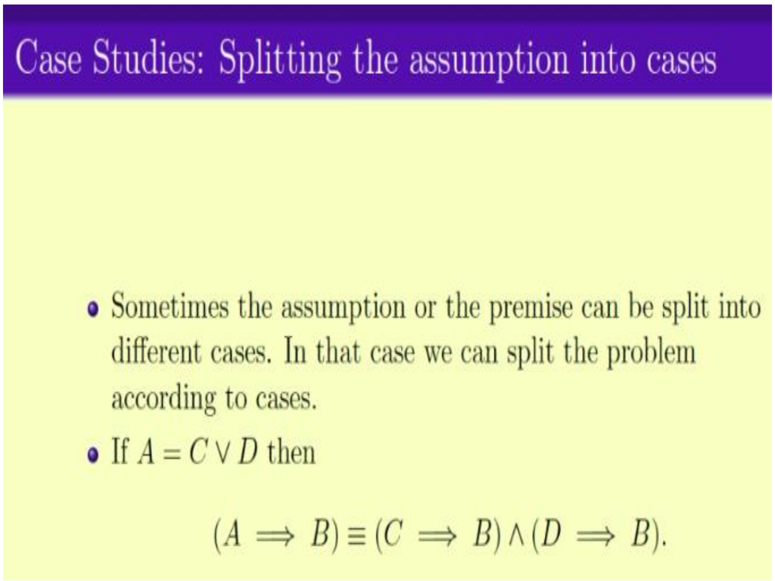
Direct proof

- 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 $\underline{C \iff B}$ then $\underline{(A \implies B)} \equiv \boxed{(A \implies C).}$

To recall, for direct proof, either you can start from A and make a step by step deduction and end up proving B, or sometimes, this direct proof can be quite magical. So we might want to come up with a different technique, the technique that we suggest it was that is going backwards. Mainly, start with B, we will start with the thing that you have to prove, work with it and slowly simplify it, to get a simplest technique, which might be real proof from A.

So in other words, if you can prove that, if you can simplify B to C, that B and C are basically equivalence statement, just that C has been more simplified in that case proving A implies B is same as proving A implies C. So working with B would help you to, working with B and simplifying A and C will help you to understand, how to finally prove A implies C. Since C is the simplifying form, so proving A implies C will be easier.

(Refer Slide Time: 08:05)



Case Studies: Splitting the assumption into cases

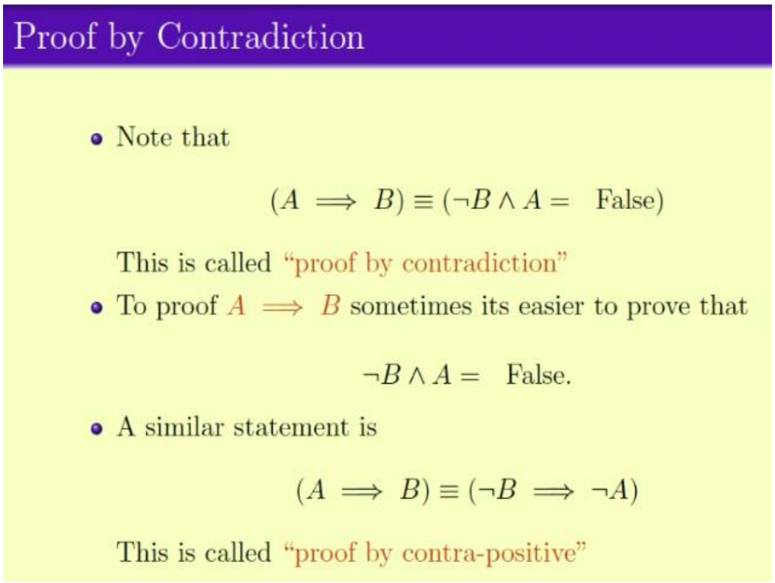
- Sometimes the assumption or the premise can be split into different cases. In that case we can split the problem according to cases.
- If $A = C \vee D$ then

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

Now, in the context of case study, the idea was that sometimes we can split up the problem into cases, depending on A. So in other words, if the statement is of the following that A equals to C or D, that means C or D implies B, then A implies B can be split up as C implies B and D implies B. Then sometime, we can split up into cases that A is either C or D and in that case, C implies B and D implies B.

We saw a couple of examples, where we use this case study to solve the problems. So this was what we did till now, namely we looked at some of the technique of splitting the problem into smaller parts and how to go about on it. On this video lecture, we will be looking at a completely new technique, which we call proof by contradiction where the idea is to view the problem in a different way.

(Refer Slide Time: 09:27)



Proof by Contradiction

- Note that

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

This is called "proof by contradiction"

- To proof $A \implies B$ sometimes its easier to prove that

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

- A similar statement is

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

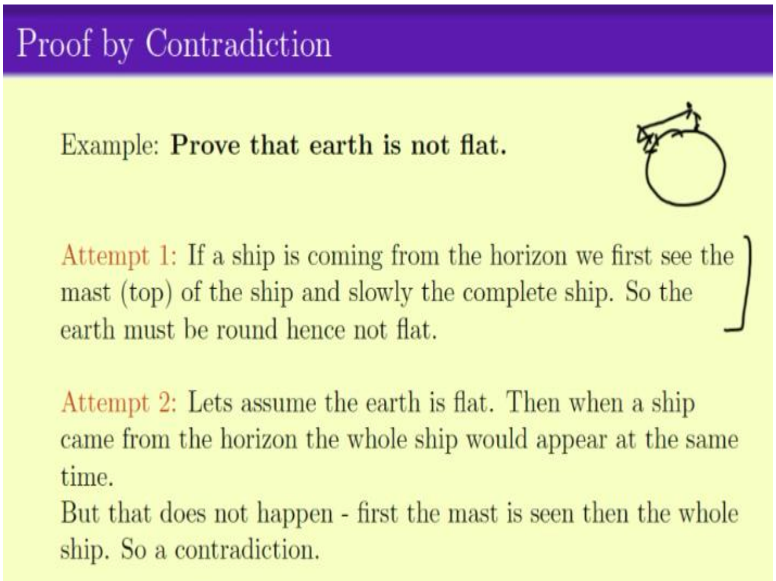
This is called "proof by contra-positive"

So, here is the idea, the idea is that, notes that proving A implies B, or this technique A implies B equifies the statement not B and A is false. So in other words, to prove A implies B, one can prove not B and A is false. This is what we call the proof by contradiction. So if you have asked that, okay, assume A and the prove B, then what you were asked to prove, what you can prove is this statement that mainly not B and A is false.

From this particular expression that we have a similar statement can be drawn, which is also of this form, that A implies B is equivalent to not B implies not A. This is called proof by contrapositive, and we will be using this technique after a couple of video. In this video, we will be looking at the proof by contradiction at this part, while we will be using not B and A is false to prove some statements.

It is a very powerful proof technique and we apply it quite a lot in our video proof mathematics.

(Refer Slide Time: 11:38)



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.

So what is that we do in the case of proof by contradiction. A good example is to consider this following example, it is not mathematical example as such, but something that is useful. Say we want to prove that earth is not flat. So, how do you prove that earth is not flat? One way of doing is that, okay, let us to prove it directly, then we say, okay, when we see a ship coming from the horizon we see first the top of the ship and slowly the complete ship arrives, right.

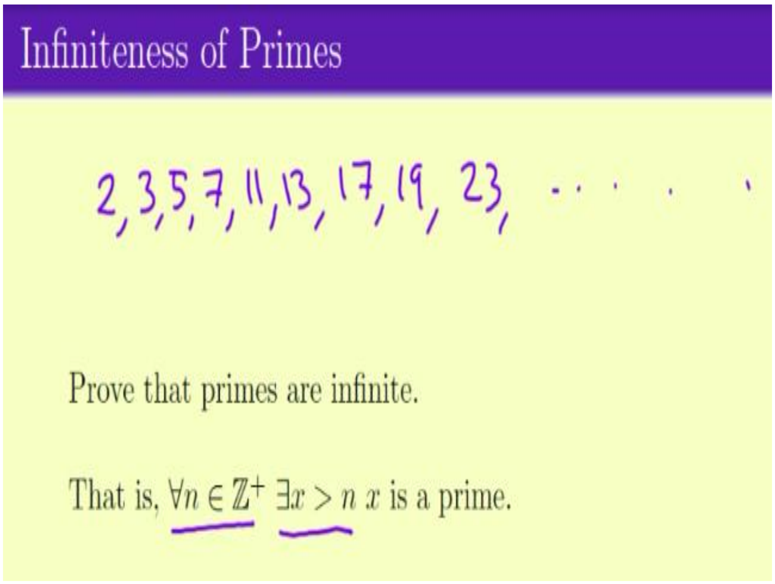
And this falls on the usual proof that we have see, that if I am standing here and say the ship here, first what we see is the top of the ship, and then much later on we see the bottom of this ship, bottom of the ship appears slowly. And the only way that it can happen is that, if it is not flat. This is the first technique that one can apply. This is what we call as the direct proof technique, which is the direct proof or the constructive proof.

The second way of saying is that, okay, let us assume that the earth is flat. In that case, there is something weird happens, we get a false statement. So, if the earth is flat, the ship is coming from the horizon the whole ship will appear at the same time. But that does not happen, we see the mast first, and then the whole ship, and hence we get a contradiction. Although, the two statements almost look so much similar, but the main thing is how it is presented at very different.

It is also tells us something important, namely these proof techniques are not necessarily written on stone. A single problem can have multiple different proof techniques. Now, all we are saying is that here there are different types of proof techniques, and you can choose any one of them. And for particular problems obtaining a proof using one proof technique might just be easier than obtaining a proof using other the technique.

And that is all that we saying in this different types of proof techniques, right. So in other word, proving that the earth is not flat can be done either using the constructive proof or using a proof by contradiction. So let us see an example.

(Refer Slide Time: 15:00)



Infiniteness of Primes

2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Prove that primes are infinite.

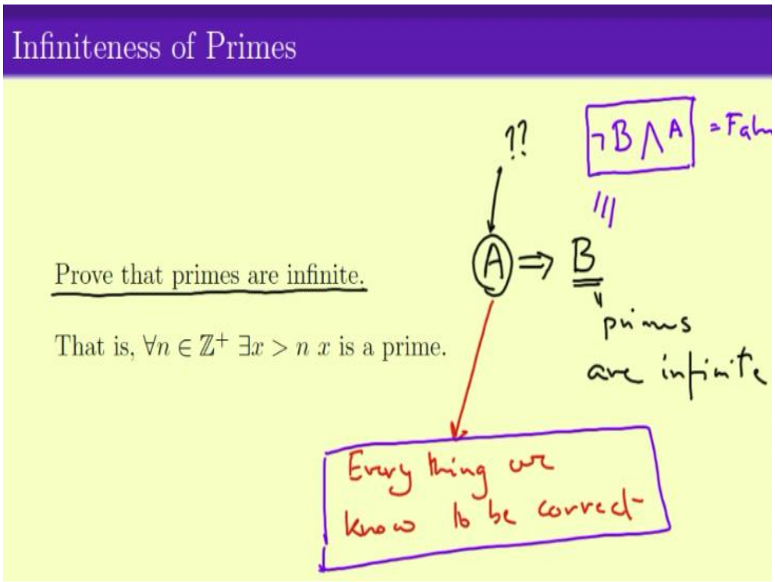
That is, $\underline{\forall n \in \mathbb{Z}^+}\ \underline{\exists x} > n\ x$ is a prime.

To see the example, you have to consider primes, and you have to prove that, the primes are infinite, in other word there are infinitely many primes. So in other words what you have to proof, you have to proof is that for all n greater than or equal to okay, so let us see an example, so consider this problem of primes. Now what are primes? We know primes are numbers that cannot be divided by any other integer less than zero.

So what are the prime that we know off? The prime that we know of are 2. 3. 5. 7. 11, 13, 17, 19, 23, and so on. Now is it that there is only a finite the prime, for example there are only 1000 primes or 10,000 primes or something like that or is it that there is always some prime. In other words, we have to prove that there are infinite number of primes. In other words, you want to say that the primes are not bounded by these large number.

So for all n, positive integer n, there always exist a number, which is bigger than n and it is prime, so these are prime that is always bigger than n, so you can pick your favourite n, so you tell me, okay. Is there are prime bigger than 10 lakhs and I should be able to be produce you one. So this proves that the number of prime are not bounded by a large enough integer, then it is fine.

(Refer Slide Time: 17:29)



Infiniteness of Primes

Prove that primes are infinite.

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

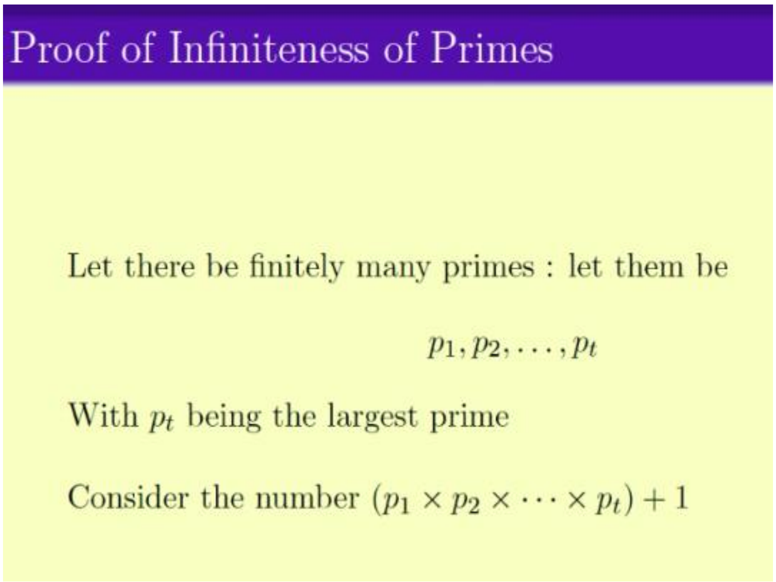
?!
$\boxed{\neg B \wedge A}$ = Fals
|||
$A \Rightarrow B$
primes are infinite
Every thing we know to be correct

Then how you proof this statement, how do you prove that the number of primes is indeed infinite. So to prove that we will prove it using contradiction. So first of all, let us go back on straight what is A, if you want to formulate this statement, that prove primes are infinite, if I have formulated in terms of A implies B and what is B and what is A. The B is here. The B is prime are infinite and what is A and as such no A here.

So many times, you will get such kind of questions. A in this case is actually everything that we know to be correct everything we know to be correct. So in fact it basically states that with all the knowledge that you have can you prove primes are infinite. So if I have to prove this statement, you can give contraindication how unequal are they. So what we are going to do is, remember, we have to prove that this whole thing is combo into not B and A. This is false, right.

In other words, this statement states that if number of primes is not infinite or in other words if the number of primes are finite, then something that we know must be contradicted. There is something that we know must have a contradiction, right and this is how we will go about proving our statement.

(Refer Slide Time: 20:20)



Proof of Infiniteness of Primes

Let there be finitely many primes : let them be

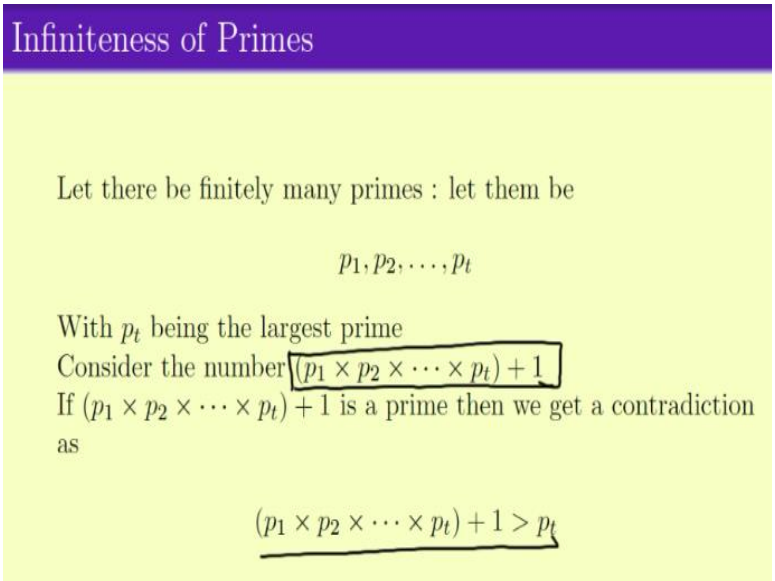
$$p_1, p_2, \ldots, p_t$$

With p_t being the largest prime

Consider the number $(p_1 \times p_2 \times \cdots \times p_t) + 1$

So let us continue with the proof. So let us assume that there finitely many primes. So that means, there is a largest prime, let us call that one pt and in that case, if the set of total primes is p1 to pt, p1, p2, p3. Now consider this number the product of all these primes plus 1. Now, what is this number? First of all, note that this number is strictly bigger than pt, why? If you remember that we know that p1 is 2, we know p2 is 3 and so on.

(Refer Slide Time: 21:24)



Infiniteness of Primes

Let there be finitely many primes : let them be

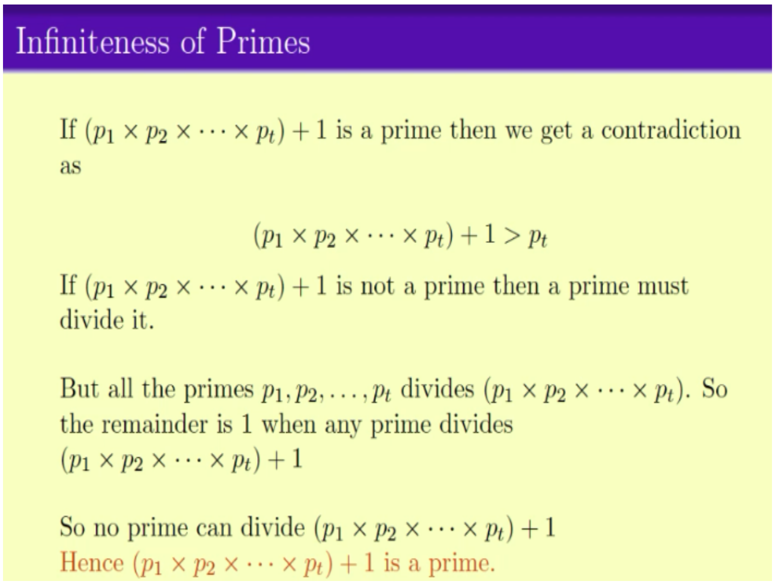
$$p_1, p_2, \dots, p_t$$

With p_t being the largest prime
Consider the number $\boxed{(p_1 \times p_2 \times \cdots \times p_t) + 1}$
If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime then we get a contradiction as

$$\underline{(p_1 \times p_2 \times \cdots \times p_t) + 1 > p_t}$$

So this number p1 times p2 and times dot, dot, dot, till pt is bigger than twice or 6pt and so on, right, so that number, this number product of all the pt plus 1. If this 1 turns out to be a prime, then what happens? This contradicts the statement first of all that pt is the largest prime. We assume pt is the largest prime, so it contradicts the statement pt is largest prime, because this is one is really greater than pt.

(Refer Slide Time: 22:21)



Infiniteness of Primes

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime then we get a contradiction as

$$(p_1 \times p_2 \times \cdots \times p_t) + 1 > p_t$$

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is not a prime then a prime must divide it.

But all the primes $p_1, p_2, \dots, p_t$ divides $(p_1 \times p_2 \times \cdots \times p_t)$. So the remainder is 1 when any prime divides $(p_1 \times p_2 \times \cdots \times p_t) + 1$

So no prime can divide $(p_1 \times p_2 \times \cdots \times p_t) + 1$
Hence $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime.

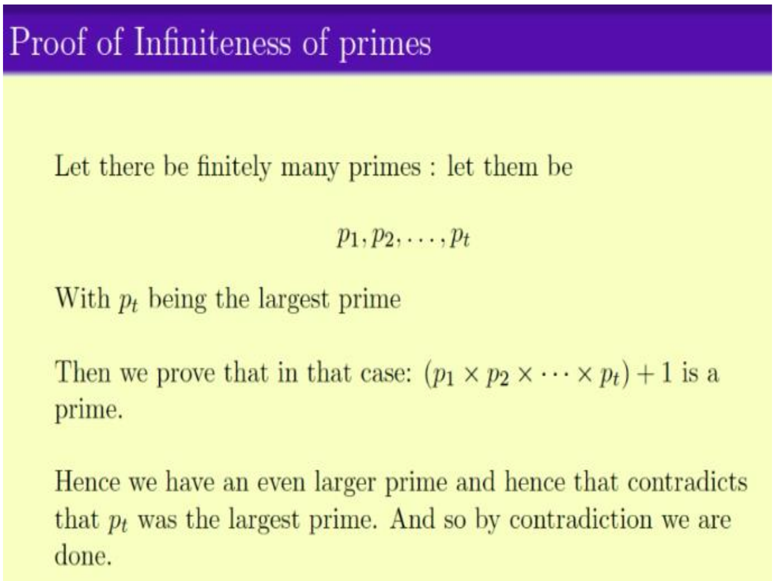
Now can or if the product of p1 to pt plus 1 a prime? Now if the product plus 1 is not a prime, then by the definition of a prime, something must be dividing it and when something divides it, we have looked at this proof earlier, that is some number integer divides another integer, then there must be a prime that divides here. So in other words some n of p1 to pt must divide this some because you want pt in the set of primes that we have.

But all the primes p1 to pt divides, of course the product of them, so when we define the product plus 1, this number, by any number, say, does p1 divides this number, when you divide this number by p1, what is the remainder? The remainder is 1, similarly when it is divided by p2, the remainder is 1, similarly with divided by the prime pt, the remainder is 1 or in other words, none of this primes p1 to pt divides this new number.

So this number is not divisible by any of the old primes p1 to pt. What does it mean? It means that, there is only one that this number has to be a prime. There is no number, no prime can divide this number and this one is a prime and this is the contradiction as we have discussed earlier, because now we have a number that is a prime bigger than the largest prime, which cannot be.

So this proves that our initial assumption of pt be the largest prime, is false. In other words, it cannot be a largest prime or other words, pt cannot be, or number primes cannot be finite.

(Refer Slide Time: 25:06)



Proof of Infiniteness of primes

Let there be finitely many primes : let them be

$$p_1, p_2, \ldots, p_t$$

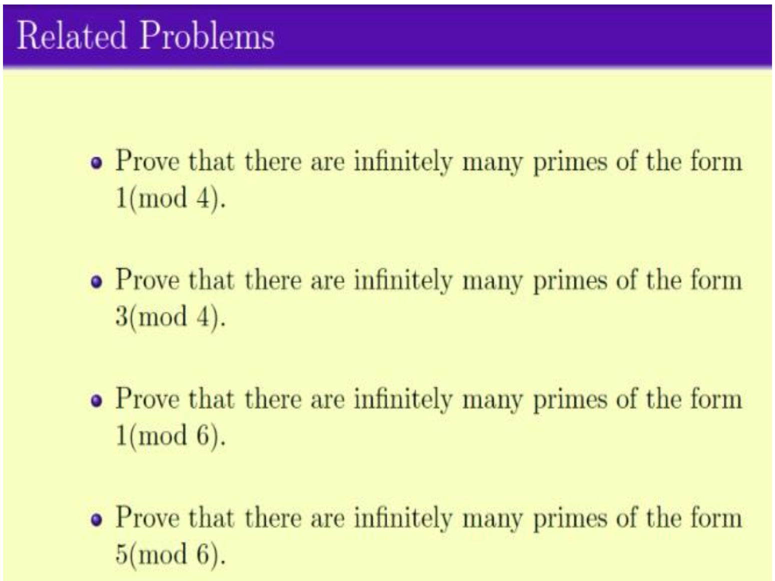
With p_t being the largest prime

Then we prove that in that case: $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime.

Hence we have an even larger prime and hence that contradicts that p_t was the largest prime. And so by contradiction we are done.

So basically, we proved that if p1 to pt are the set of primes, finite set of primes, then I created a new number because larger than largest prime and we prove that has to be prime, which is a contradiction. So this is a typical proof by contradiction where we start from assuming that the statement that we have to prove is not true and we worked our way through and at the end proved that it contradicts something, either it contradicts what you are assuming or it contradicts something that we know and so on.

(Refer Slide Time: 26:04)



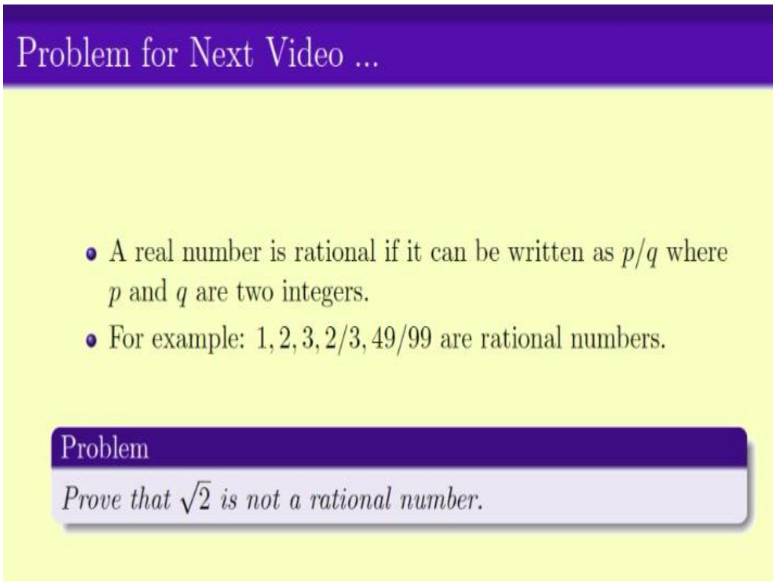
Related Problems

- Prove that there are infinitely many primes of the form 1(mod 4).
- Prove that there are infinitely many primes of the form 3(mod 4).
- Prove that there are infinitely many primes of the form 1(mod 6).
- Prove that there are infinitely many primes of the form 5(mod 6).

There are many related problems to this particular problem and I leave it to you for exercise for you to prove that there are infinitely many primes of the form 1(mod 4). So mainly what are the primes 1(mod 4), same thing, 5, 13, 17, 29 and so on. Prove that there are infinitely many primes of the form 1(mod 4). Similarly prove that there are infinitely many primes of the form 3(mod 4).

Again, similarly prove that there are infinitely many primes of the form 1(mod 6) and there are infinitely many primes of the form 5(mod 6). So we will be doing some more problems using contradiction in the next video.

(Refer Slide Time: 27:10)



Problem for Next Video ...

- A real number is rational if it can be written as p/q where p and q are two integers.
- For example: $1, 2, 3, 2/3, 49/99$ are rational numbers.

Problem

Prove that $\sqrt{2}$ is not a rational number.

So in the next video, we will be proving some statements like the square root of 2 is not a rational number. What is a rational number? A real number is rational if it can be written as ratio of two integers. So if a number can be written as p/q where p and q are integers, then we say this is a rational number and 1, 2, 3 they all can be written as 1/1, 2/1, 3/1, 2/3, 49/99 and so on. We claim that square root 2 is not rational.

In the next video, we will be proving this particular problem using the same contradiction technique. I encourage you guys to go and try to solve this problem by yourself before you see the next video. Thank you.