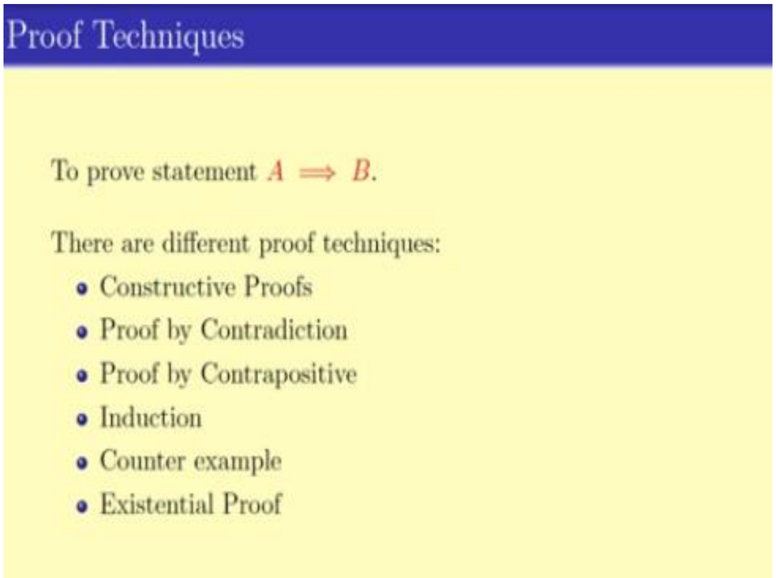
Discrete Mathematics
Prof. Sourav Chakraborty
Department of Mathematics
Indian Institute of Technology - Madras

Lecture - 08
Proof Technique (Case Study)

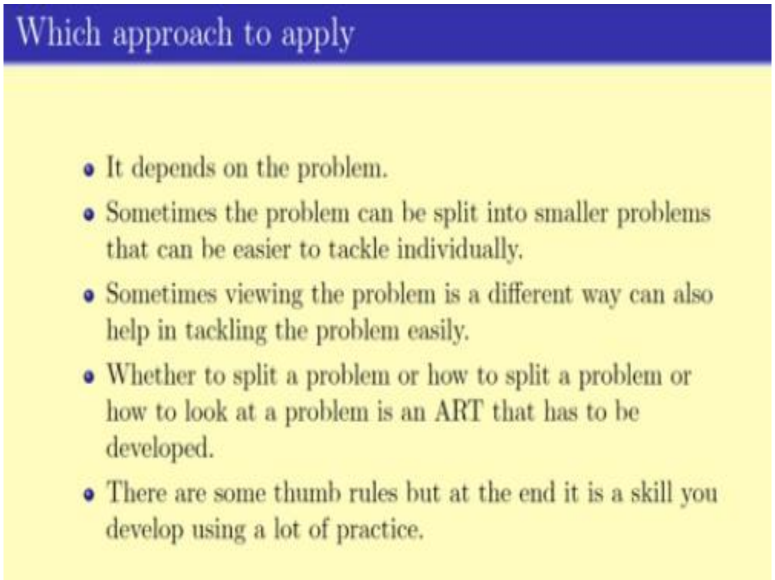
Welcome everybody to the eighth video lecture in discrete mathematics, so today we will be continuing our study in the proof techniques and particularly in the constructive proofs and we will be looking at the case study proofs.

(Refer Slide Time: 00:16)



So to recall, so we want to prove a statement B from statement A and there are various proof techniques that can be applied namely Constructive proof, Proof by Contradiction, Proof by Contrapositive, induction, counter example and Existential Proof. We will be looking at this various proofs one by one; currently we are looking at the Constructive proofs.

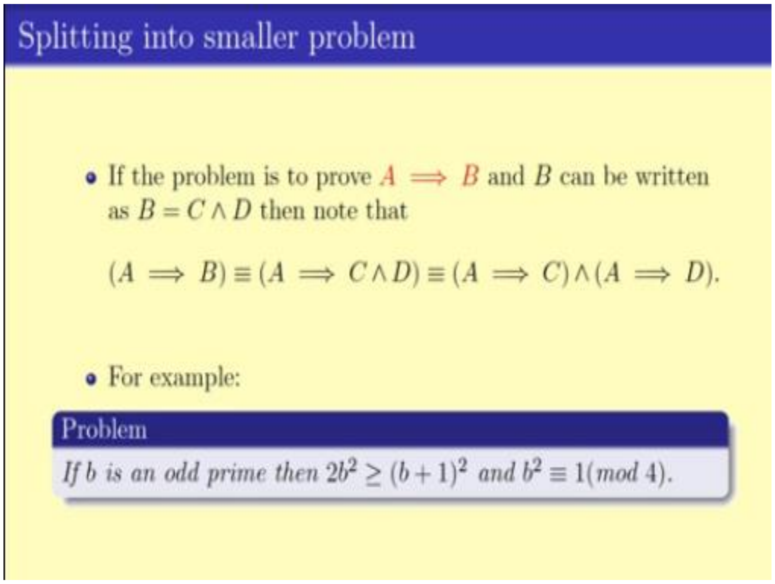
(Refer Slide Time: 00:40)



This problem comes again and again to your mind and hence I will repeat it every video talks video lecture where we talk about this proof techniques namely which of these approach to apply and let me tell it once again that it depends on the problem, which some for some problems you might be able to apply a particular technique and for some problem some other technique, some problem can be split into smaller problems that can be handled easily, while some problem can be viewed in a completely different way, which can help us in understanding the problem easier.

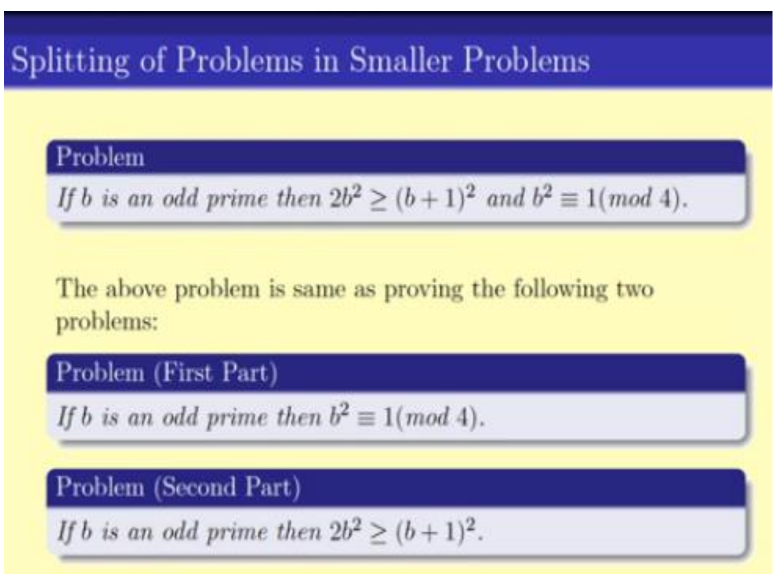
But whether to split a problem or not and how to split a problem and how to look at a problem this is an art itself and that has to be developed by you. There are some thumb rules that we can provide you. We will be teaching you the various technique and telling you the thumb rule, but at the end of the day, it is you who have to develop the skill of understanding, which problem will require which application and that can be achieved only by a lot of practice.

(Refer Slide Time: 02:01)



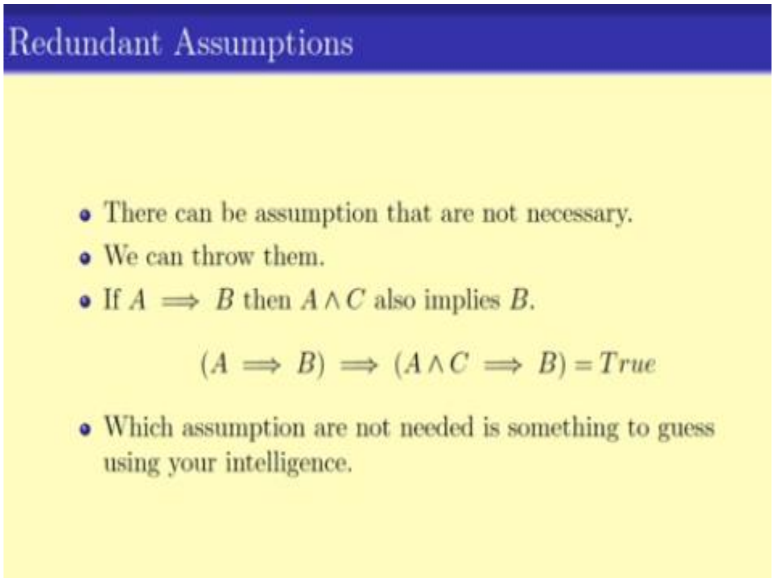
Now till now, we have seen things like how to split a problem into 2 smaller parts, if the deduction that we make with an and, that means if we have proved A implies B and B can be written as C and D then A implies B is basically same as saying A implies C and A implies D, so we saw the example, which was saying that b is an odd prime then 2b square is greater than or equals to b + 1 whole square and b square is congruent to 1 mod 4 and applying this particular splitting this problem into 2 parts depending on the deduction.

(Refer Slide Time: 02:51)



We could split them into 2 parts, namely first part if b is an odd prime then b square is congruent to 1 mod 4 and the second part if b is an odd prime then 2b square is greater than or equal to b + 1 whose square.

(Refer Slide Time: 03:15)

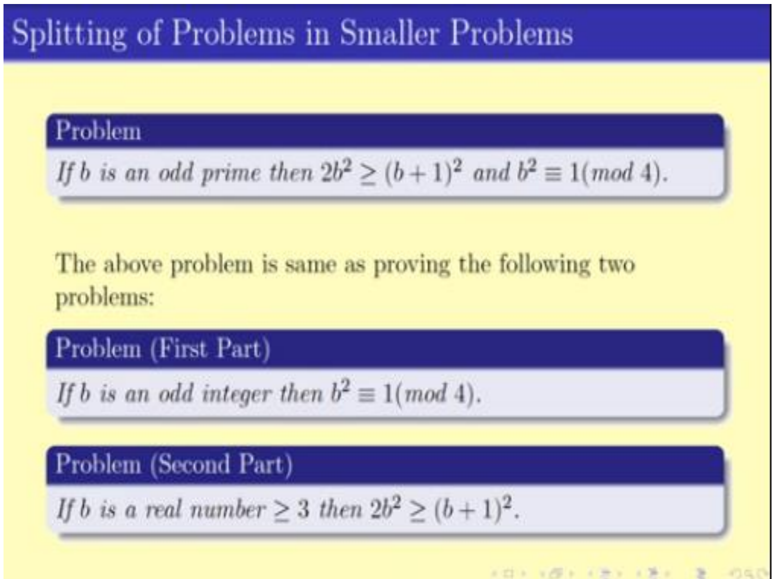


Now moving on, we also saw that there can be Redundant Assumptions namely there can be some assumptions that are not necessary, then keeping those assumptions can only make the problem more confusing and complicated, so if we can throw them away it would be a big advantage for us. For example, if we can prove A implies B and the assumption says that you can assume A and C.

And clearly this assumption C is a return in assumption that basic idea is that if A implies B then A and C also implies B, so the original problem was actually A and C implies B, then you can say flip away C and solve the problem of A implies B, that might help you to simplify the problem make your understanding clearer and it will be a useful thing to do. Now which assumptions that are needed and which assumptions are not needed, which assumptions should be thrown and so on.

All depends upon your intelligence, in sense that your experience and intelligence will tell us, which one will be required which one will not be required.

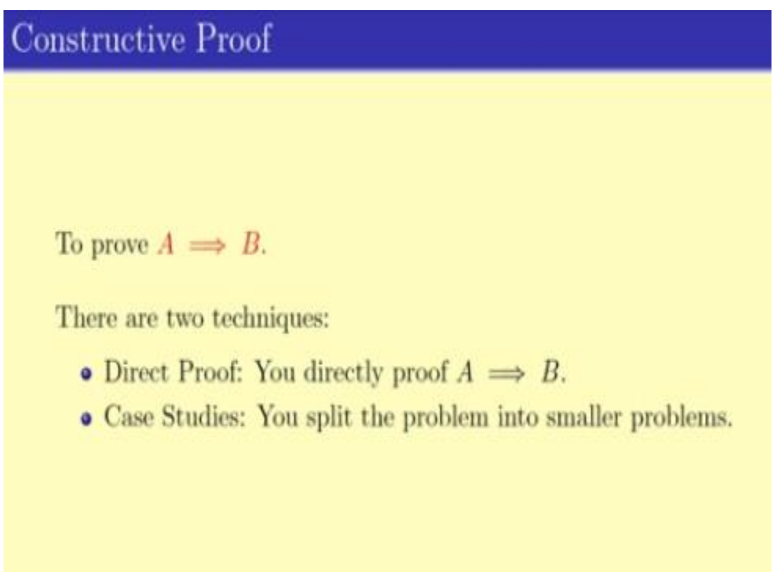
(Refer Slide Time: 04:51)



We saw the application of this particular thing in our problems, namely we had these 2 problems, part A and part B and we apply this both of them into this particular removing of redundancies in assumption, in particular we looked at with what property of the odd prime given the fact that B is an odd prime what property of the odd prime do we need in either of the cases and what we realized is that in the first case all we need is that b is an odd integer.

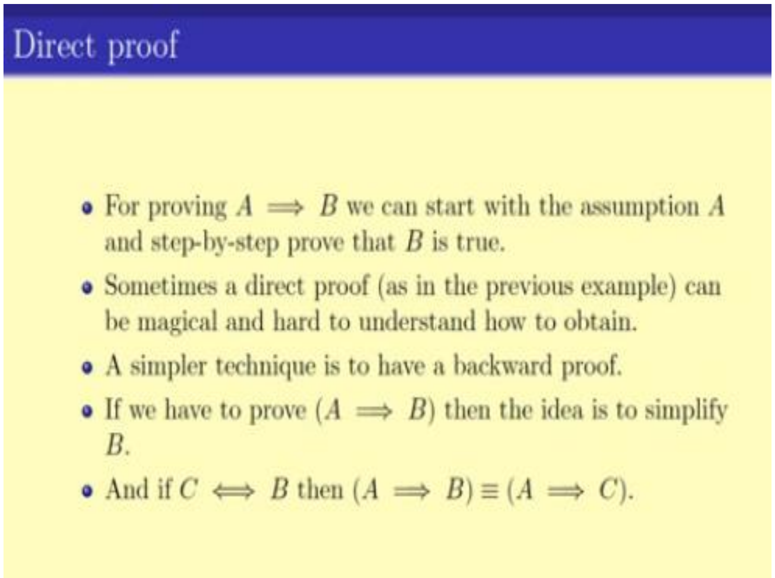
And second case, all we need is a b is a real number greater than or equals to 3 is a typical example of problems of where redundancies in the assumptions are not required.

(Refer Slide Time: 05:42)



Now, we continued from here and solved these 2 problems using direct proofs, so we used direct proof which is a special case of the constructive proof and as I told you earlier, constructive proofs have 2 parts, part A it is what we call as a direct proof that means you directly prove A to B or in other words you message A to get B, the second one is case studies and I will come back to this one particularly in the end of this video lecture.

(Refer Slide Time: 06:17)

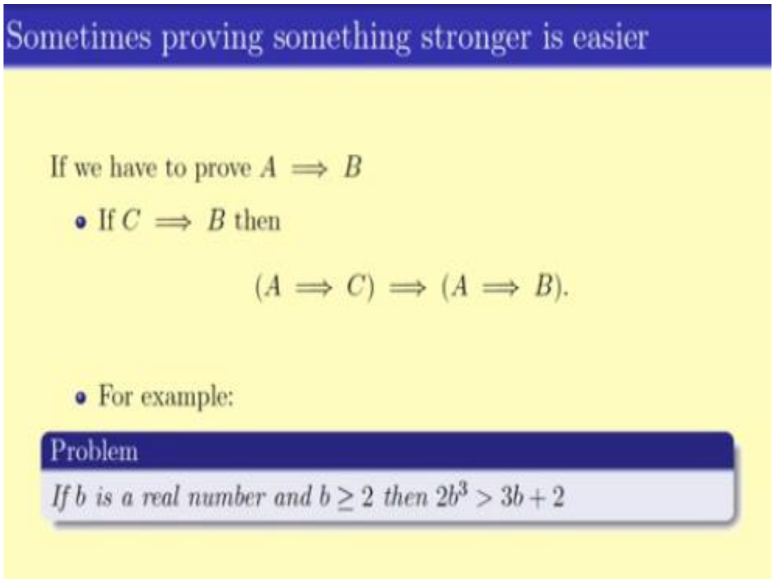


So we had used this direct proof for proving our 2 problems, so we gave you 2 problems namely 2 problems and 2 different approaches the first approach was okay work with A, keep on working with A and whatever else is known to you and you can output B, by you can deduce B by doing a step-by-step deduction.

The other option is going in the backward direction it is because sometimes direct proof can be a bit magical and confusing we have seen this particular example earlier in the earlier video where direct proof is not very clear how to obtain a direct proof, so in that case we would like to use a backward proof, now what is the backward proof?

The backward proof is nothing but you start working up your way through B in other words to prove A implies B, the idea is to simplify it can we say okay we have to prove A implies B now what does B mean and let us keep on simplifying this problem and basically it turns out that if you can finally prove that B and C are same in that case A implies B is of course same as say A implies C and now that you have simplified C it might help you to understand or get a full proof of A implies B or C directly, so that is the idea of the direct proof either you go forward or go backward, so this is what we did till last video.

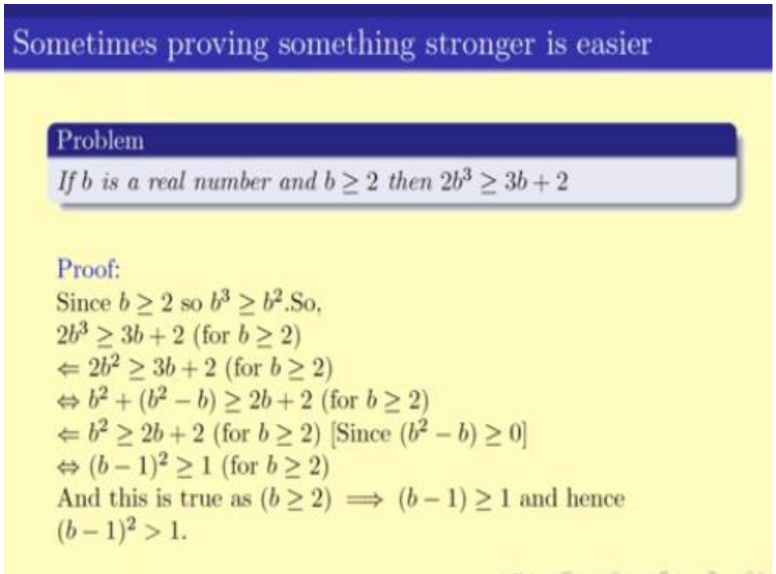
(Refer Slide Time: 08:21)



Now this video let us start with one more special case that can arise, namely sometimes prove your proving something that is stronger can be easier, now what do we mean by that? Say we want to prove A implies B, but I know that C implies B, so if I can prove A implies C, then I may be able to prove, sorry if I can prove A implies C then immediately it will imply A implies B. Now the catch is that C can be a much stronger statement than B.

It is possible that C is much stronger so you might not be able to prove A implies C, so I am actually asking you to prove a harder statement to obtain A implies B, but that does not happen sometimes, namely sometimes we do come across problems where proving something harder can actually be easier, so let us look at this 1 example. So here is an example it says that if b is the real number and b is greater than are equals to 2 then 2b cube is strictly greater than 3b + 2.

(Refer Slide Time: 09:59)



Now how to prove this number? Let us see, so first of all we know that B is greater than or equals to 2 that means b cube is greater than or equals to b square. These only follows from the fact that P is greater than equals to 1 actually and now since this is true therefore 2b cube. So to prove 2bq is bigger than or equals to 3b + 2 this is what we have to prove, to prove this line.

It is this line it is follows from the fact that if we can prove 2b square is greater than or equals to 3b + 2. Note hear that this statement that 2b square is bigger than or equals to 3b + 2 is actually a harder statement to prove, but we are saying that okay, if we can prove the harder statement then the previous statement which is what we want will follow. So the implication here is not if and only if unlike we want a saw in the last case when we are removing assumptions.

But here we are making the problem or our goal harder and harder now to prove 2b square is greater than or equals to 3b + 2, this is same as of course b square plus, now I have just basically taken the b in the other side, so b square + b square - b is greater than or equals to 2b + 2. Now once again note that this b square - b is greater than 0, why? Again by the same logic that since b is greater than 2.

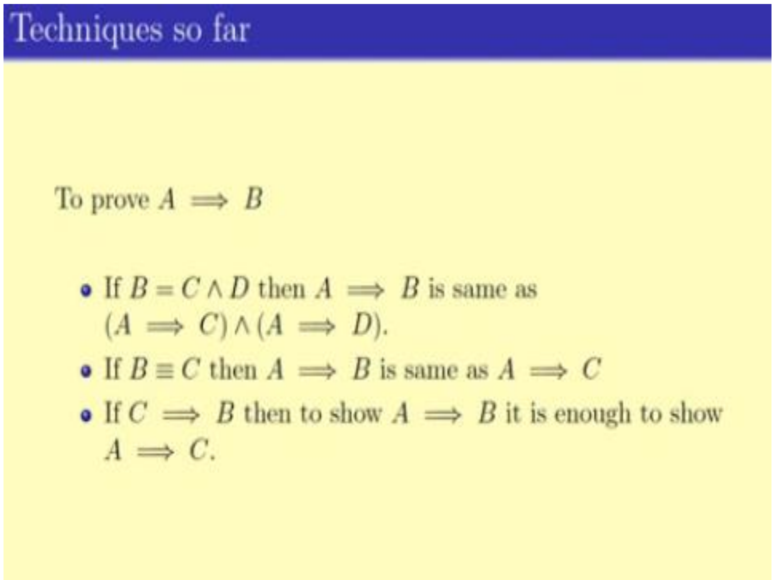
So, b square is greater than b so b square - b is greater than 0 that means, I can remove this positive term on the right hand side, sorry on the left hand side, in other word I am saying is remove a positive term and still can you prove this statement b square is greater than or equals to

2b + 2, again note that this line is actually a harder line to prove than the previous line. But the reason I am doing it is that this line now as you can see looks much more tractable.

It does not have a cubic expression and its pretty neat at this point and as you can kind of guess here that this is doable in the other words, so this follows from the fact that b - 1 whole square is greater than or equals to 1, from which it follows that this follows from the fact that if b is greater than or equals to 2 we have the result, right. So in other words, we could go in the we could go in the backward direction or not backward direction rather we could simplify make our problems harder and harder and yet at the end, we could get a solution.

The reason is that once we make the expression doable, it was easier for us to prove, although the problem as such become harder, the trick here is that there are hard problems or harder problems and then there are problems which you can solve. Sometimes solving a harder problem can be easier and hence converting a simpler problem to a harder problem can mean the actual trick right, okay.

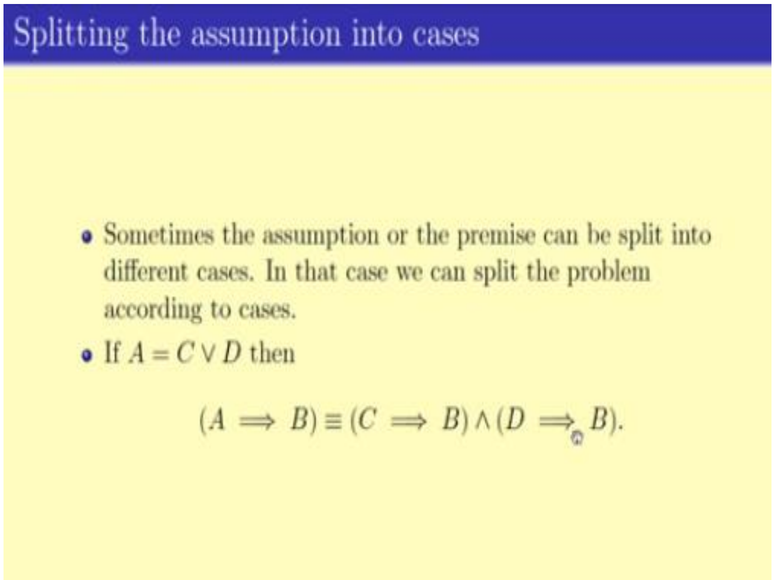
(Refer Slide Time: 14:36)



So moving on, so the techniques so far that we have seen till now is to prove A implies B, we can either split up the problem into 2 smaller parts depending on whether B can be split up as C and D, we can see that if we can reduce the reduce B or not reduce we can find out a C which is same as B then proving A implies B is same as proving A implies C. We also prove that if C implies B.

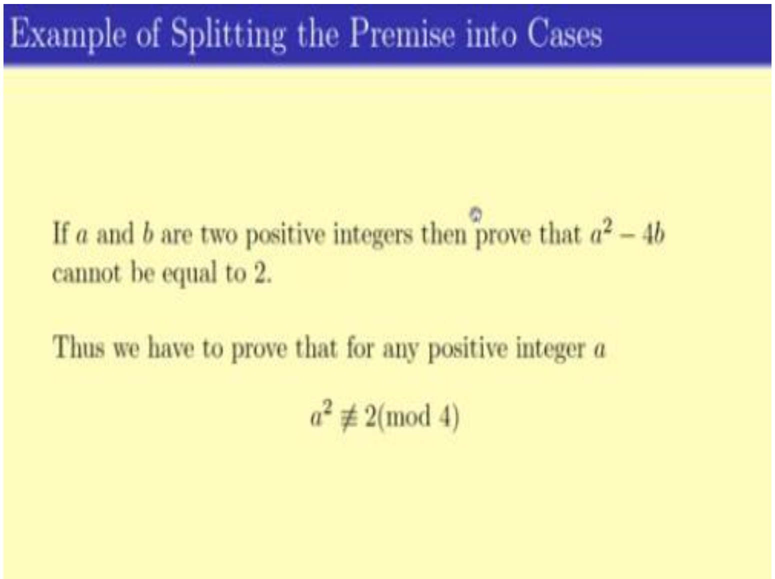
And we can imply, we can prove A implies C then this is enough to prove A implies B that means making it harder can be actually easier sometimes. So this is the kind of the technique that we have learned so far. Now in the rest of the video, I will be going into a new way of splitting the problem this depends on splitting it according to the assumptions.

(Refer Slide Time: 15:52)



So in other words sometimes the assumptions can be split into different cases and in that case we will be able to split it up into smaller problems, for example again if we have to prove A implies B and A is C or D, then A implies B is same as saying C implies B and D implies B. Please prove it for yourself that this statement is indeed correct use the propositional logic technique that we have done to check that this is indeed correct.

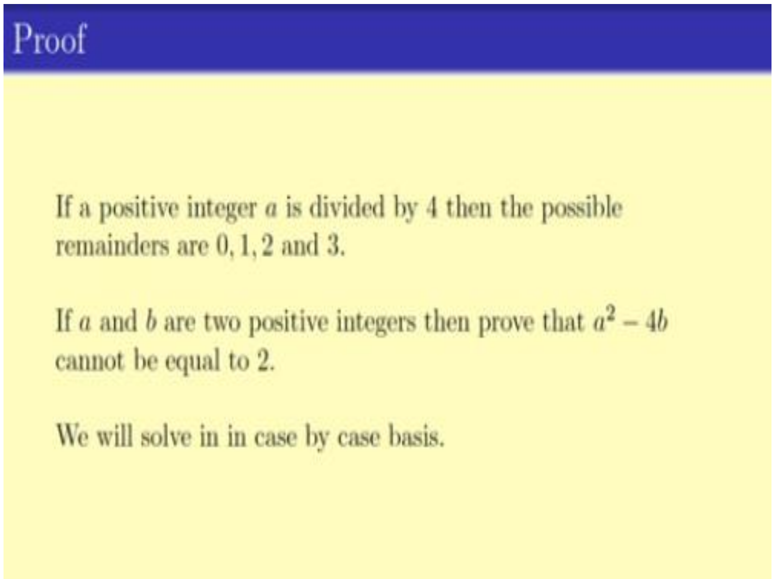
(Refer Slide Time: 16:39)



So for example, let us start with this example that we have here if A and B are 2 positive integers then prove that a square - 4b cannot be equals to 2. How do you split this problem? First we have to understand what is the a and what are the b, now what is the a here, the a or set of assumptions is a and b are 2 positive integers okay. There is does not seem to be a very natural way of splitting it up or is it okay, we will see and what is the deduction?

Deductions is that a square - 4b cannot be equals to 2. Now this is what we do okay. So this is another way of stating it that is this problem is says that a square is not congruent to 2 mod 4, recall your number theory notations that if I say that a square - 4b cannot be equals to 2 which means that a square - 2 is not divisible by 4 or a square is not congruent to 2 mod 4.

(Refer Slide Time: 18:08)

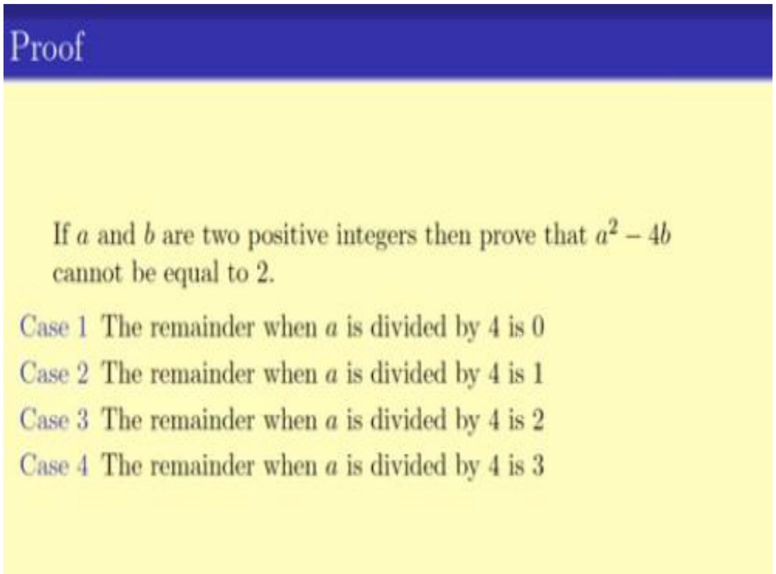


Now to start with the proof as I told you, I would like to split the assumptions in 2 cases. Now this is the first of its kinds may be you are seeing and therefore I am going to do it fully here. I will give you a few set of problems on this line that you will be asked to solve for your exercise, and you will also of course you will also get an assignment at the end of this week, which will include all this kind of questions on this subject.

So one way of splitting it up is that, what are, so if A is the positive integer and if divide by 4, what are the possible remainders? And possible remainders are of course 0, 1, 2, and 3 right. So if I have to prove this particular statement that is if which is basically means that a square is not congruent to 2 mod 4, then it is the same as we can solve it by case by case basis or in other words, we can say that okay, let a be a, let a be the integer that is divisible by 4 or which means that the remainder is 0.

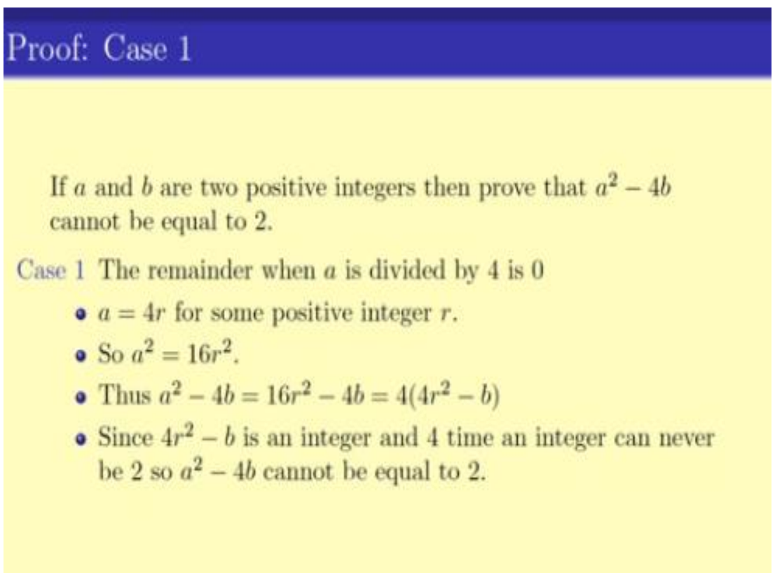
Then can I prove it? Secondly second case will be if a when divided by 4 has reminder 1, can I prove it? That will be second case. Third case and fourth case similarly for remainder 2 and 3. So that is basically the plan. So we split the problem into 4 cases depending on the name remainder when a is divided by 4.

(Refer Slide Time: 20:12)



So if the case says are and I told you case 1, case 2, case 3 and case 4 depending on the remainders of 0, 1, 2 and 3. Now when we have this, we can do a case by case basis, so we can take the case 1 and solve it.

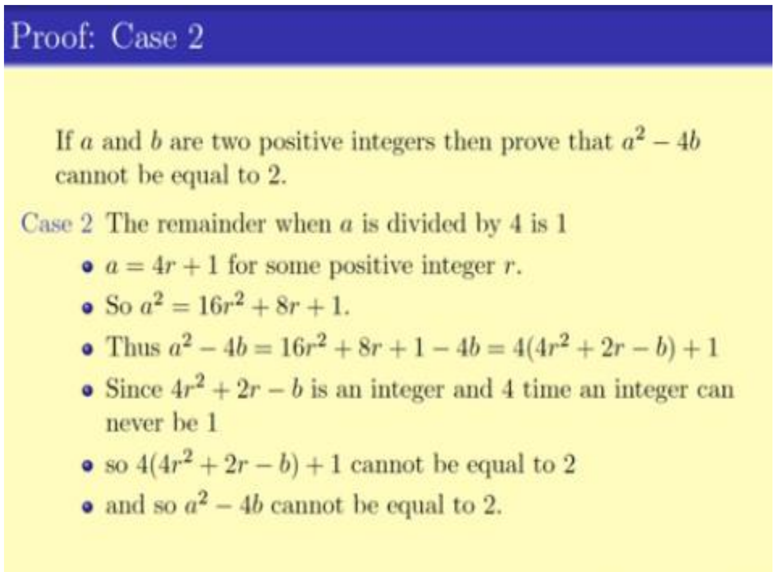
(Refer Slide Time: 20:32)



So let us start with it, so the case 1 we know that the remainder when divided when a is divided by 4, it has remainder zero or in other case a is equals to 4r for some positive integer r. Now let us see in that case can you prove something that a square is congruent not congruent to 2 mod 4 possibly let us see. So a square is equals to 16 r square just by squaring it and therefore, if I take any 4b so a square - 4b is 16 r square - 4b which is 4r square - b.

Now since 4r square - b is an integer and 4 times an integer can never be equals to 2, therefore 4 into 4r square - b can never be 2 or in other words a square - 4b cannot be cannot equals to 2 in this particular case. So this prove us that if a is divisible by 4 or if a has remainder zero when divided by 4, then we prove that a square - 4b cannot be equals to 2. Now you can, you do not need to look at the rest of the video at all. You can just try to solve your problem by you can solve the other cases other 3 cases by yourself.

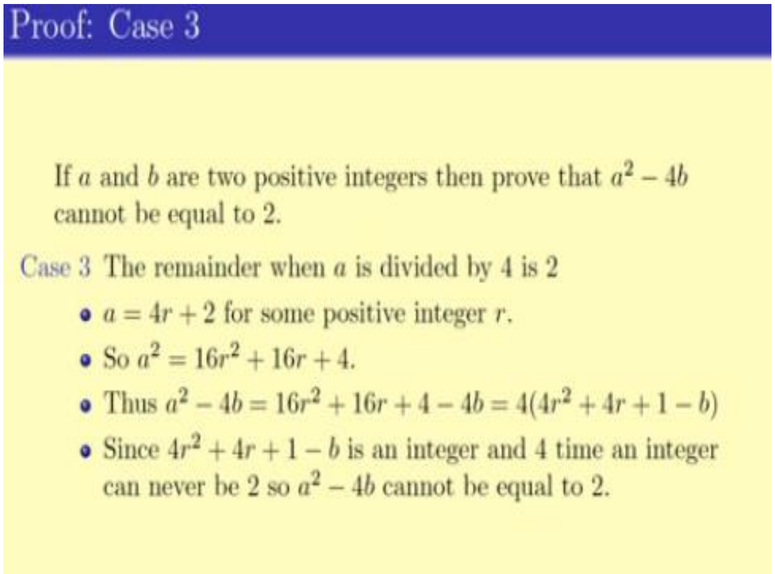
(Refer Slide Time: 22:28)



For example, for the case of case 2 that is the very remainder is 1, then what can we say again we can say that a is equals to 4r + 1 for some positive integer r, again let us do it what is a square a square is 16 r square + 8r + 1, so a square - 4b will be 4 times 4r square + 2r - b + 1. Now you can already see that this is a 4 times a number + 1. So this is an odd number. This is not an even number because 4 times a number is an even number + one it is odd number.

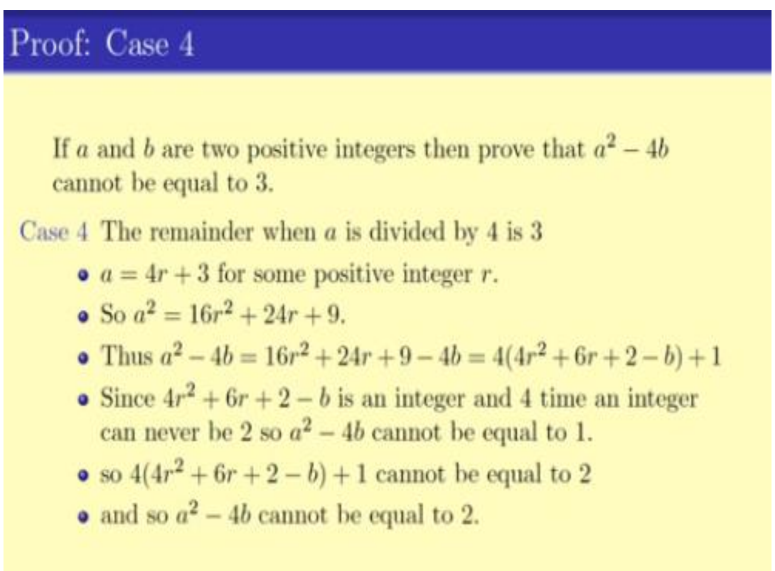
Thus this number just can now never be 2, the same way of saying is that, that is 4 times this number can never be 1 and so we have that a square - 4b cannot equals to 1 even in this case.

(Refer Slide Time: 23:53)



Let us go to the case 3, in the case of case 3 the same thing. We start for the case where is a, is a has remainder 2 when divisible by 4 in that case a is equals to 4r + 2 for some positive integer r, now if we square it up we get some 16r square + 16r + 2 actually that is right, they have done it right and now if I do this a square - 4b this is 4 times 4r square + 4r + 1 – b, which is again if you realize same things as the first case where it is 4 times an integer and hence cannot be equals to 2 right. This is again a 4 times integer and hence cannot be equals to 2.

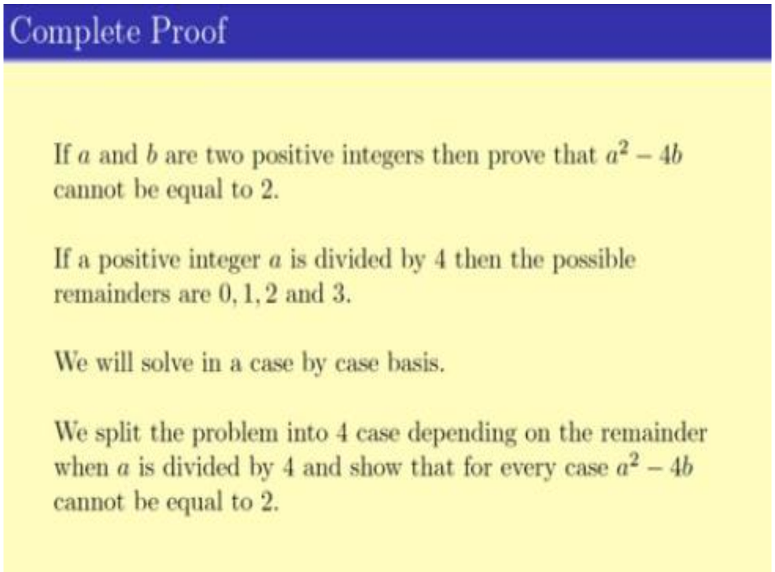
(Refer Slide Time: 24:54)



Now, this brings us the last case, which is the case where the remainder is 3 again here a is equals to 4r + 3, so a square is 16r square + 24r + 9, now here if I subtract it, you have to break this line as 8 + 1 and then you realize that this is 4 times 4r square + 6r + 2 - b + 1, again it is the

4 times the number integer + 1 and hence this cannot be equals to 2. Thus we have broken up into 4 cases and for each of the cases we have proved that this statement a square - 4b cannot be equals to 2, so this concludes the whole proof.

(Refer Slide Time: 25:49)



So to complete the proof we first ensure that we split up the assumption into 4 cases. Now this is something very important we have to ensure that this 4 cases are the only cases can there be any other cases? No in this case, it is very easy to convince that there is no other case, so in other words if a is positive integer, then when it is divisible by 4 the only remainders left are 0, 1, 2 or 3. Thus, we have exhausted all the cases.

This is a very important thing to check always in case studies whether all the cases have been considered and then we solve the problem in a case by case basis, right and we proved there for each of the cases it cannot be equals to 2. So this is a typical case study problem where we split the assumptions or split the problem depending on the assumptions. We will see more of this particular technique in the next video also okay. So this brings us to the end of this video lecture. Thank you.