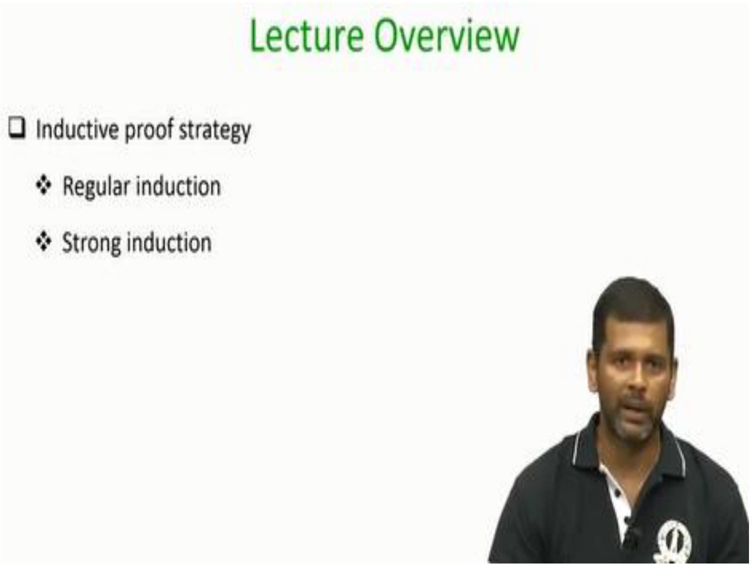
Discrete Mathematics
Prof. Ashish Choudhury
Department of Mathematics and Statistics
International Institute of Information Technology, Bangalore

Lecture -12
Induction

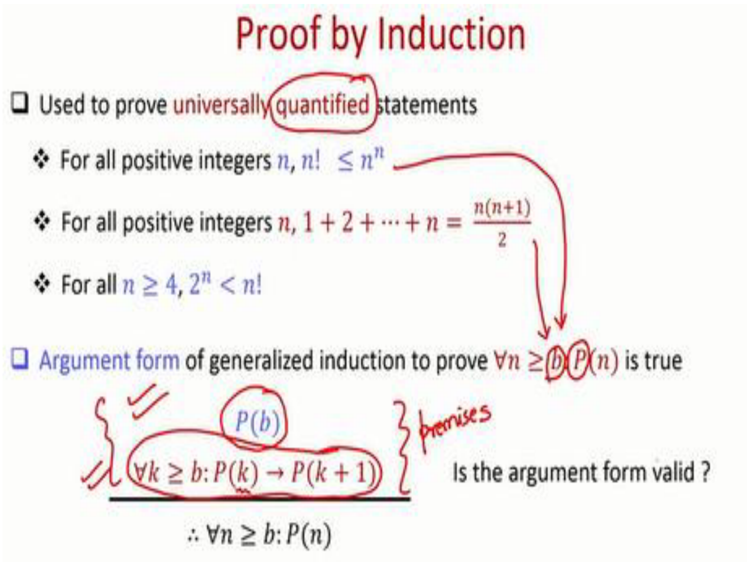
Hello everyone. Welcome to this lecture on proof by induction.

(Refer Slide Time: 00:32)



So just to recap in the last lecture we have we started discussing extensively about various proof mechanisms, which we used to prove different kind of statements. In this lecture, we will continue our discussion on proof strategies and we will introduce a very important proof mechanism namely proof by induction which we will be using extensively in this course. We will be seeing two forms of proof by induction namely proof by regular induction and proof by strong induction.

(Refer Slide Time: 00:57)



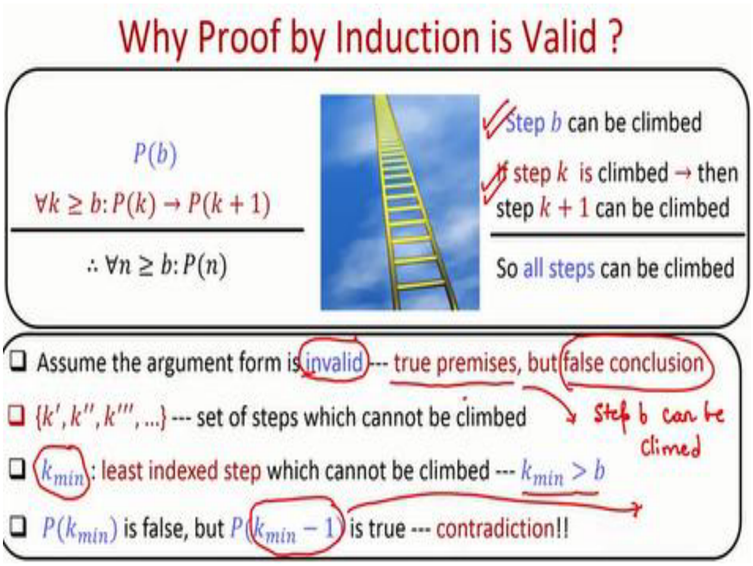
So what is proof by induction? So you must have encountered proof by induction several times. It is generally used to prove universally quantified statements namely statements of the forms such as for all positive integers n factorial is less than or equal to n^n. For all positive integers n and the summation of first n numbers is $\frac{n(n+1)}{2}$ and so on. So it is used to prove all this universally quantified statements and what is the argument form of induction proof?

So imagine P is a property or a predicate and you want to prove that the property P is true for all values of n starting from b onwards. So for instance, if I take the first statement here, the property P here is that n factorial is less than equal to n^n, that is the property P and we want to prove it is true for all positive integers. In the same way for the second statement a property P is that summation of 1 to n is $\frac{n(n+1)}{2}$ and so on.

So there will be some base case or some starting value and we want to prove that the property P is true for all values of n starting from b onwards. So the argument form for the proof by induction is as follows. So, these are your premises, namely it will be given to you or you will be proving explicitly that the property P is true for the element b in the domain. So the proposition P(b) is true and you will also prove that for any k greater than equal to b if the property P is true for the element k in the domain then the property P is true even for the element k + 1 in the domain.

So based on these two premises a proof by induction concludes the conclusion that the property P is true for all n greater than or equal to b. So now the question is this argument form valid? Because that is what we typically do in proof by induction, in proof by induction these are the two things which you prove. You prove what we call as the base case and then we prove the inductive step and based on that we conclude at the property based P is for all n greater than equal to b. So the question is that is this a valid proof mechanism is this argument form valid or not.

(Refer Slide Time: 03:28)



So to understand that why prove by induction is a valid proof mechanism, let me give you an analogy. So you imagine that you have an infinite ladder and I want to make the conclusion that all steps of the ladder starting from b onwards can be climbed, if these two premises hold. So, what are the two premises here? It is given to me that definitely you can climb step number b and it is also given that, if you can climb step number k then it is guaranteed that you can climb step number k + 1.

So these are the two conditions given to you and my claim is that if these two conditions are true then I can conclude that all steps starting from b onward can be climbed, that is what is an analogy for proof by induction. So the property P in this example is that you can reach step number x or step number b or step number k. So; the property that I want to prove here that you can reach all the steps here.

So the way we prove that proof by induction is a valid proof mechanism is as follows. So assume that the argument form of proof by induction is invalid and from the definition of invalid argument this means that I have true premises that means, the statements in the premises are true, but the conclusion is false. If that is the case that means there are definitely some steps which cannot be climbed.

So say these are the set of steps which cannot be climbed and this set exists because I am assuming that the conclusion is false. So since the conclusion is false that means definitely there is at least one step which I cannot climb and there might be many such steps. So I am a numerating all such steps which are unreachable. Now among these steps, I focus on the least indexed step, which cannot be climbed and I call it k_{min} and again this index k_{min} is well defined because this k_{min} is the least value from a set of values.

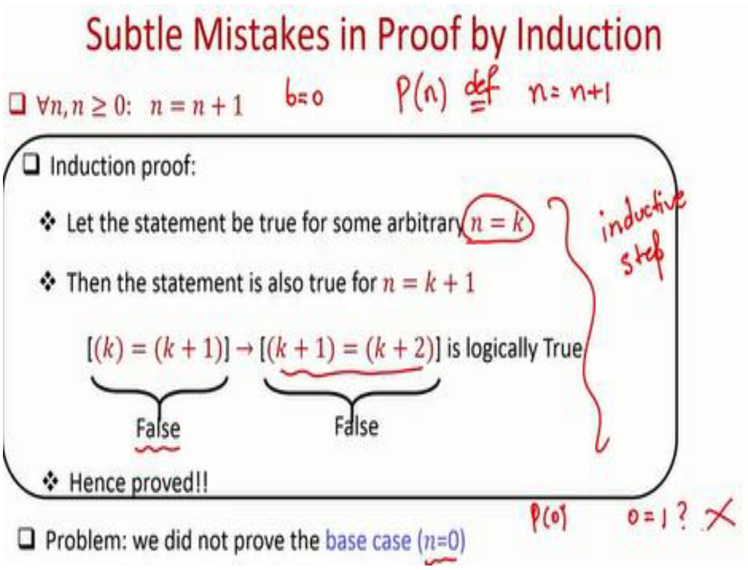
Now, I can say that definitely k_{min} is greater than b this is because I am assuming my premises are true and my premises are true means step b can be climbed; that means that is a true statement, that means definitely k_{min} cannot b. So k_{min} can be anything after b onwards, but if the property P is false for k_{min}; that means if the step number k_{min} is unreachable; that means the step number $k_{min - 1}$ is reachable; or the property P is true for the element, $P(k_{min -1})$.

But this gives a contradiction, because if step number $k_{min - 1}$ is reachable; then since my premises are true; it gives me the guarantee that step number k_{min} can also be can be reached that means the property P is true even for the element k_{min}, because my premise is true but then it is not simultaneously possible that k_{min} is true as well as k_{min} is false that means whatever I assumed, that means, I assumed that means my assumption that argument form is invalid is an incorrect assumption and that means the proof by induction is a valid proof mechanism.

So that is a very simple proof that indeed just by proving these two statements, you can come to the conclusion that the property P is true for all values, all values starting from b onward. So in the proof by induction the starting case is called as the base case, that means the first few values for which the proposition of which is the predicate is true, though they are called as the base cases.

There may be multiple base cases; we will see, it is not necessary that there is just one base case and the second premise that you are proving here is the inductive step. Where assuming that the property P is true for any value of k starting from greater than equal to b onward. You prove that the property P is true even for the next element of the domain that is inductive step.

(Refer Slide Time: 09:10)



It turns out that very often people make subtle mistakes in proof by induction. So here let me demonstrate one such subtle mistake. So imagine my property P is that P(n), my property P(n) is that n is equal to n + 1 and I am making a universally quantified statement that the property P is true for all values of n greater than equal to zero. So my base case here is zero. Now, suppose someone tries, but definitely this is a false statement, here is the induction proof, which is given in an attempt to prove this statement to be true.

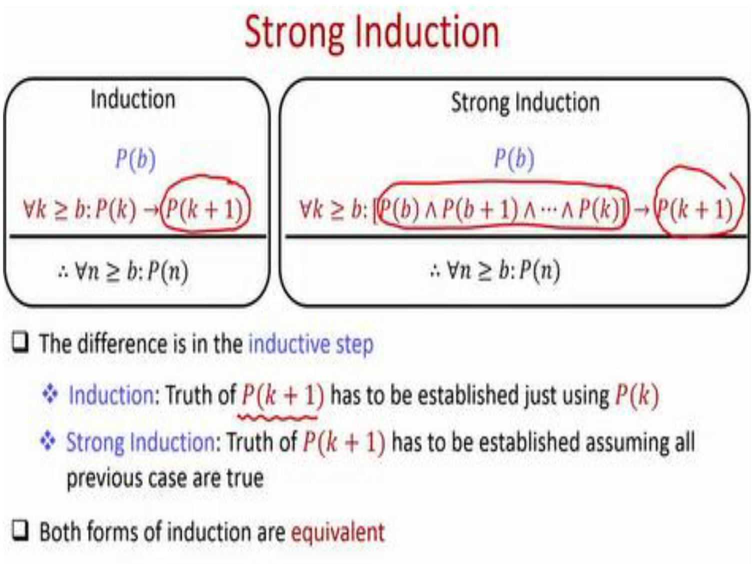
So, let the statement be true for some n equal to k; that means we are proving trying to prove the inductive step then the statement is also true for n equal to k + 1 and why so because if the statement is true for n equal to k, so that means P(k) is true and P(k) is nothing but the proposition k is equal to k + 1 and we want to prove that the statement is true even for k + 1 and the predicate P(k+1) is nothing but the proposition k + 1 equal to k + 2 and if you see this implication is logically true because P(k) is false.

Why P(k) is false? Because k is not equal to k + 1. So I have false here my premise is false and if my premise is false over all the implication will be true that means assuming the statement is true for n equal to k and I am able to show that the statement is true for n equal to k + 1 as well. Now since we have proved the inductive step you might be wondering whether we have proved that the statement is true for all values of n.

Well, the mistake in this proof is that you have not proved the statement for the base case; you have just proved the inductive step here. Assuming that the property P is true for n equal to k you have proved at a statement is true even for n equal to k + 1, but what about the base case? There is no starting case for which you have proved the property to be true. You have not proved the statement to be true for the base case and the base case here is n equal to zero and proposition for the base case n equal to zero or P(0) is the statement that zero equal to one which is definitely a false statement.

So, that is why this is an incomplete induction proof, you just prove the inductive step you have not proved a base case and that is why this proof is not acceptable.

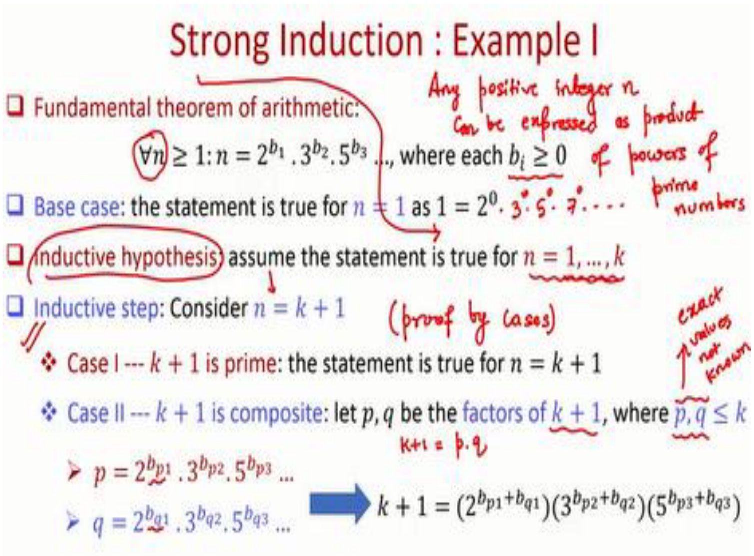
(Refer Slide Time: 11:58)



It turns out that there is another form of induction, which we call as strong induction. So this is your argument form for the regular induction where you are given a base case and in the inductive step assuming that, the predicate P is true for k you prove it to be true for k + 1. In the strong induction, the difference is in the inductive step. So the difference is that in the regular induction, the truth of the proposition P(k+1) has to be established by just using P(k) that means when you want to prove that P(k+1) is true, you are just given the hypothesis or the premise that P(k) is true. You are not told anything about what is P(k – 1), P(k – 2) and so on. Whereas in the strong induction, which we have for which argument form is given in the right hand side part when you are establishing the truth of proposition P(k+1), while doing that you can assume that the statement P is true for all values in the domain starting from b up to k that is the difference. The difference is in the inductive hypothesis.

However it turns out that both forms of induction are equivalent that means if you have a proof by regular induction, then you have proof by strong induction for the same property P, whereas if you have a proof by strong induction for the property P, then you can find an equivalent proof for the same property P, but using regular induction. We will prove we will establish this equivalence towards the end of this lecture but you might be wondering that why, what some motivation of strong induction.

(Refer Slide Time: 13:57)



The main motivation of strong induction is that it simplifies your proofs several times. In many cases, it is possible that you cannot apply the regular induction directly, but by using strong induction, using the help of strong induction the proof is simplified a lot. So let me demonstrate this. I prove what we call as the fundamental theorem of arithmetic and the fundamental theorem of arithmetic says that you take any positive integer starting from one onward it can be expressed as product of prime factors or prime powers, basically.

So what the state informally the statement here is any positive integer n can be expressed as product of powers of prime numbers and if you are wondering what are prime numbers, well a number is prime if it has no divisor other than the number itself and one, other than the number itself and one. So, this is the formal statement, if you want to prove this statement and we will prove this statement using induction and we will be using strong induction.

So since this is a universally quantified statement, we have to prove a base case and we have to prove the inductive step. The base case is when n is equal to one and it is easy to see that if n is equal to one then one can be written as 2^0. I stress here the statement does not need that b_2, b_3, b_4, everything should be 1, the powers of prime it can be zero as well. So I can express 1 as 2^0 and if you want you can further write it as 3^0, 5^0 and so on that means the base case is true.

Now I go and prove the inductive step and while proving the inductive steps since I am using strong induction, my inductive hypothesis will be that assume that the statement is true for all values of n or all integers n from one to k onwards; I do not know what exactly is the prime power factorization of 1, 2, 3, 4 up to k, I do not know the exact prime power factorization, but I am just assuming that this statement is true for all numbers in the range 1 to k.

And now assuming this, I have to show that even the statement is true for n equal to k + 1 as well. This is your inductive step. Now there can be two cases possible with respect to k +1. So now you can see that I am applying here proof by cases. So within the inductive step, I am applying the proof by cases depending upon whether k + 1 itself is a prime or it is a composite number. So there can be only two possibilities.

If k + 1 it is a prime number then my statement is true because I can write k + 1 as k + 1 raise to power 1. Thats all, into of course 2^0, 3^0 and so on. So that means my statement is true for n equal to k + 1 whereas case two could be where my k + 1 is a composite number that means it has some divisors and let p and q be the factors of k + 1. Now since p and q are factors of k + 1 both of them are upper bounded by k.

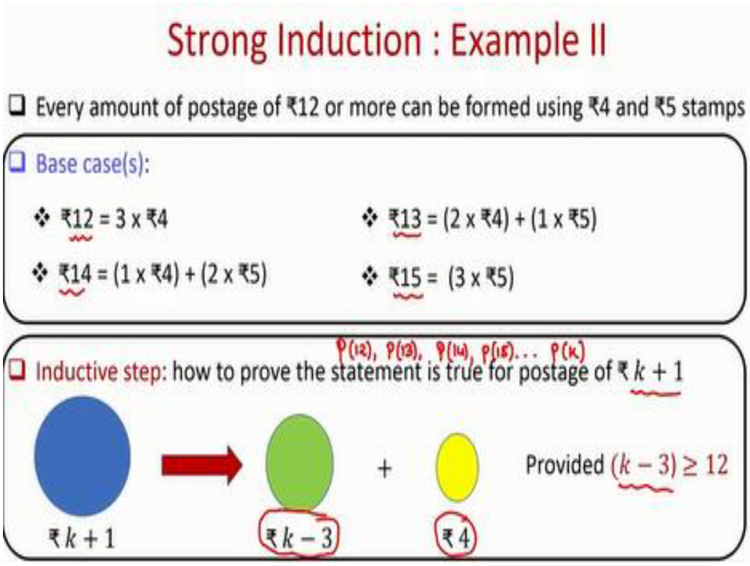
It cannot be possible that p is k + 1 or q is k + 1 because if p is k + 1 that means the number itself is a factor of itself which implies that k + 1 is a prime number not a composite number. Since it is a composite number its factors will be definitely less than equal to k. But I do not know the exact values of p and q, I just know that factors p and q exist, the exact values not known. But I know the range of p and q because k + 1 is an arbitrary integer here.

Now since p is less than or equal to k and q is less than or equal to k and in my inductive hypothesis I am assuming that the statement is true for every value of n equal to 1 to k, that means the statement is true even for p and the statement is true even for n equal to q. Since the statement is true for n equal to p, that means the number p has a prime power factorization that means it can be expressed as product of powers of prime.

I do not know what exactly are those prime powers, but I know it is expressible as product of prime powers. So let this expression be the prime power factorization of p and in the same way since the statement is true for n equal to q that means the number q also has its own prime power factorization. Now based on this, since my k + 1 is equal to p times q because p and q are factors of k + 1, I can say that the prime power factorization of k + 1 can be obtained by combining the powers of two from the individual factorizations of p and q. Similarly, combining the powers of three from the individual factorizations of p and q and so on, that means I have proved that even there exist a prime power factorization for the integer k + 1 and that proves my inductive step. So, you can see that how the strong induction simplifies my proof.

The reason I am using strong induction is because I do not know the exact values of p and k, I cannot say that definitely p is k or q is k say p is k by 2 and q is something else. In that case, if I am trying to give a regular induction proof, I cannot use the fact that the statement is true only for n equal to k, I need here the fact that the statement is true for all values of n up to k and that simplifies the proof a lot.

(Refer Slide Time: 20:37)



Let me give you another example of strong induction and a statement here is imagine that in India the only postal stamps which are issued are of denomination rupee 4 and rupee 5. Now the statement I am trying to make here is that each denomination or each postage of rupees 12 or more can be expressed in terms of only 4 rupees stamp and 5 rupees stamps that is the statement I am making here.

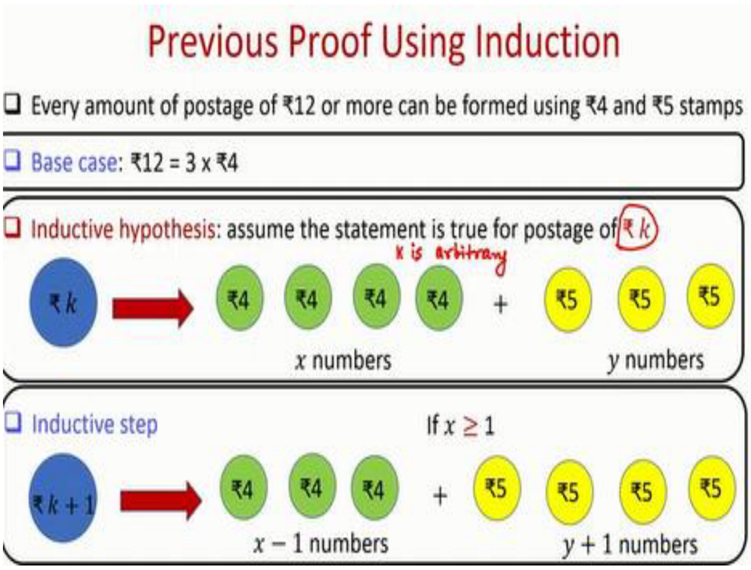
So here my base cases will be as follows; I have four base cases, and you might be wondering why four base cases it will be clear very soon. So, I am showing here that if you have an amount of rupee 12, then you can express it by taking three stamps of 4 rupee. If you have an amount of 13 rupees, then you can represent it by taking two stamps of 4 rupee and one stamp of 5 rupee and in the same way you can represent any you can, represent a denomination 14 and you can represent the postage amount of 15, so that these are my base cases.

Now I want to prove the inductive step where I want to prove that the statement is true for k + 1 assuming that the property P is true for 12, assuming that the property P is true for 13, the property is true for 14, the property is true for 15 and the property P is true for any denomination equal to k. Assuming all these things I have to show that the denomination k + 1 is also expressible in terms of 4 rupee stamp and 5 rupees stamp.

So the idea here is that the postage of k + 1 can be written as summation of postage for k - 3 and a 4 rupee stamp, that means you take one 4 rupee stamp and whatever way you can represent the postage of k - 3 to that representation, if you add a stamp of 4 rupee denomination, then you can get a representation for postage for k + 1 and this works provided k - 3 is greater than equal to 12 that means your k - 3 has to be 12 and that is why we have here four base cases.

If you do not have four base cases here, if you have say base case of only 12 then this proof does not work. So now you can see that how the proof is simplified if I assume a strong induction proof and I have multiple base cases.

(Refer Slide Time: 23:35)



What I will do is I will show that the same statement can be proved using a regular induction where while proving the inductive step I am just using the fact that the premise is true for n equal to k and here I will be just proving one base case. I do not need four base cases by base case here will be that the postage of 12 rupee can be represented by taking three stamps of 4 rupee. While proving the inductive step I assume the hypothesis that the statement is true only for postage of rupee k.

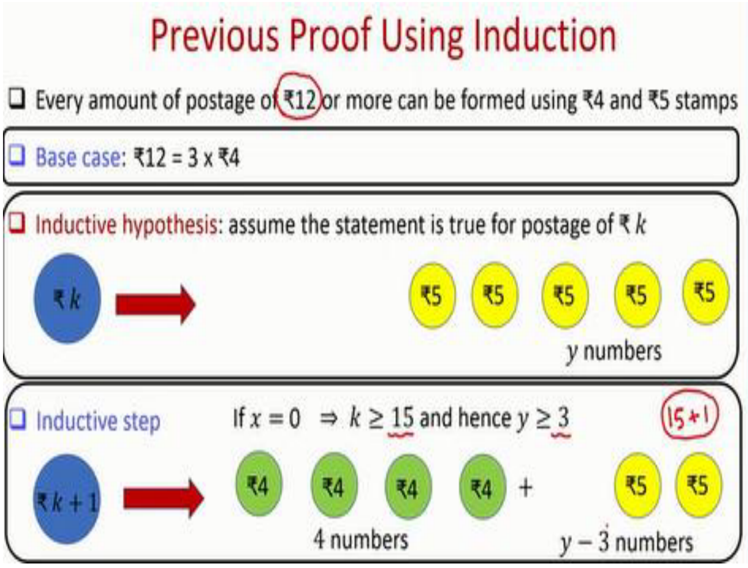
So since the statement is true for postage of rupee k that means I can represent the amount of rupee k by taking x numbers of 4 rupee stamps and say y number of 5 rupees stamp. I do not know the exact values of x and y because my k is arbitrary here remember, when I am proving the inductive step I am taking my k to be arbitrary because I am trying to prove a universally quantified statement and to prove a universally quantified statement my value of k has to be arbitrary because I will be applying the universal generalization.

Now while applying the inductive step I have to show how can I represent postage of k + 1. Now by proving that inductive step I take two cases, two possible cases depending upon whether x is zero or nonzero. If x is non zero that means at least one 4 rupees stamp was used to represent my postage of rupee k and what I can do is the following. I can take x - 1 number of stamps of rupee 4 and take y + 1 numbers of stamps of rupee 5 and that will together give me a postage for rupee k + 1.

And this is possible because I am assuming that x is greater than equal to 1. So what I am saying here is say for instance x is equal to 2 and say y is equal to 3 then instead of taking two 4 rupee stamps, now you take one 4 rupees stamps in that process now you have reduced the postage by 4 rupee and you have to take care of one rupee more because now you are trying to find a denomination of k + 1.

So you have reduced by four that means you have to take care of 4 + 1. So you have to take care of 5 rupees postage which you can take care by adding one extra stamp of five rupees to the number of stamps of 5 rupees, which you might have used for representing the postage of k rupees that is the idea here; that is case number 1.

(Refer Slide Time: 26:28)



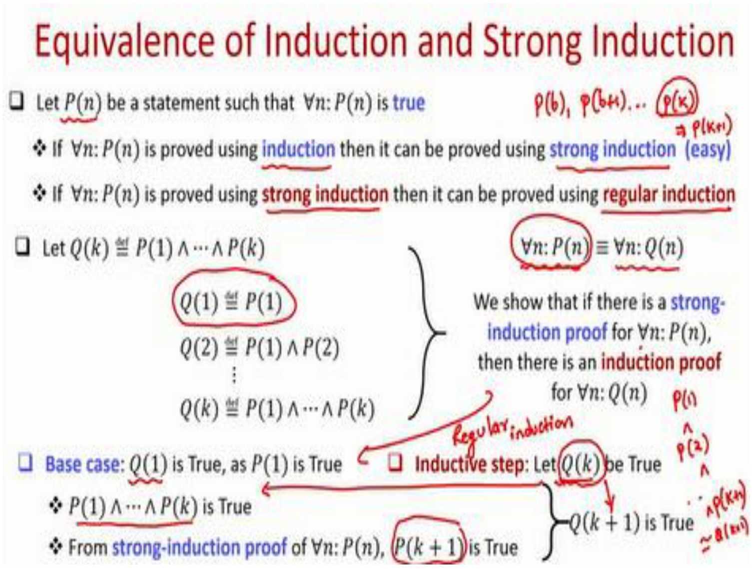
Case number 2 is; when x is zero that means when you represented the postage of k rupees no stamp of 4 rupees was used. Well, in this case what we can say is that the denomination case definitely 15 because if only stamps of 5 rupees are used to represent my amount or postage of rupee k, that means k is a multiple of 5 and the statement is for any denomination from 12 onwards.

So the smallest multiple of 5 is 15 that means my y is at least 3 here, I have at least three 5 rupee stamps which are used to represent my postage of k rupee. So what I have to do is I have to represent now a postage of k + 1 rupee. So what I can do is, instead of taking now y number of stamps of 5 rupees, I will take y - 3 numbers of 5 rupees; y - 3 numbers of 5 rupees and I will take four stamps of 4 rupee that will overall give me a postage of rupee k + 1.

And this is possible because y is greater than equal to 3. So, I can reduce the number of five rupees times by three. So the idea here is since you are reducing the stamps of 5 rupees by 3 you are subtracting 15 from k and you have to take care of one more rupee postage because you want to represent k + 1. So, you have to take care of a postage of rupee 16, which you can take care by taking or purchasing four stamps of 4 rupees that is the idea here.

So, now you can see here that in the inductive step I am just assuming that the statement is true for n equal to k, I am not using the fact that a statement is true for all n equal to 12 up to k but in that case my base case will be one and the proof will be divided into two cases which was not the case for proof by strong induction. So, depends upon your convenience if it is convenient to give proof by strong induction, you can go for proof by strong induction otherwise you can use proof by regular induction.

(Refer Slide Time: 28:47)



Now as I said earlier that any proof given by regular induction is equivalent to proof by strong induction and so on. So what we will do here is we will prove that if you have a predicate P(n) and if the universally quantified statement for all n, P(n) is true. Then we will show that any proof for proving this universal quantification by induction can be converted into a proof by strong induction and vice versa.

So one direction is very simple if this universal quantification is proved using a regular induction proof then it automatically can be treated as a proof by strong induction. Because in a proof by strong induction, you are not forced to use all the premises, namely you are not forced to use P(b) as well as P(b+1) as well as P(b+2) as well as P(k). you have free to use any of these premises to establish that P(k+1) is true.

Well, if you can just use P(k) to prove P(k+1) that is also can be created as a proof by strong induction, so this is easy. What we will now show is that if you have proved this universal quantification using strong induction, then I can find a proof for proving the same universal quantification, but using regular induction. How do I do that? So let me define a predicate Q(k) and Q(k) is defined to be the conjunction of propositions P(1), P(2) up to P(k).

So as per my definition Q(1) is same as P(1), the proposition Q(2) is the conjunction of proposition P(1) and P(2) and in the same way the proposition Q(k) is the conjunction of propositions P(1) up to P(k). From this I can conclude that the universal quantification for all n P(n) is logically equivalent to the universal quantification for all n Q(n) that means if your property P is true for all values of n in your domain then so is the property Q.

And this follows from the way I have defined my predicate Q(n). So what I will show here is; if you have a strong induction proof for proving your LHS then I can convert it into a proof or I can get a proof using regular induction to prove my RHS and since both LHS and RHS are logically equivalent that means I have now given a regular induction proof to prove my original property.

So let us see a regular induction proof for proving my universal quantification that for all n Q(n) is true. So my base case will be Q(1) and Q(1) is true because as per my definition Q(1) is P(1). And I am assuming here that there is a strong induction proof for universal quantification for all n P(n). In that strong induction prove, there will be a base case, the base case will be P(1) and since P(1) is true, I can conclude that Q(1) is true.

Now let me prove the inductive step for this regular induction proof; for the regular inductive step I will make the inductive hypothesis that Q(k) is true. I am not making the hypothesis that Q(2), Q(3), Q(4) up to Q(k – 1) is true, I am just making the hypothesis that Q(k) is true but if Q(k) is true then as per the definition it means that the conjunction of P(1), P(2) up to P(k) is true that is the definition of proposition Q(k).

And, since I have a strong induction proof for the property P, in the strong induction proof I can conclude that if P(1), P(2), P(k) are simultaneously true then the property P is true for even k + 1 that is a guarantee that the strong induction proof the existing strong induction proof gives to me.

But if P(k + 1) is also true then I can say that the conjunction of P(1) and conjunction of P(2)and conjunction of P(k + 1) is also true.

And this is nothing but Q(k + 1) that means starting with the assumption or the hypothesis that Q(k) is true, I established the truth of proposition Q(k + 1) and that means I have given a regular induction proof for proving the universal quantification involving the predicate Q. Internally while proving this implication I use the fact that I have already a strong induction proof for the universal quantification involving the predicate P.

So that brings me to the end of this lecture, just to summarize in this lecture we introduced the proof by induction mechanism, we saw two forms of induction proof namely the proof by regular induction and proof by strong induction and we also discussed that they are equivalent to each other. Thank you.