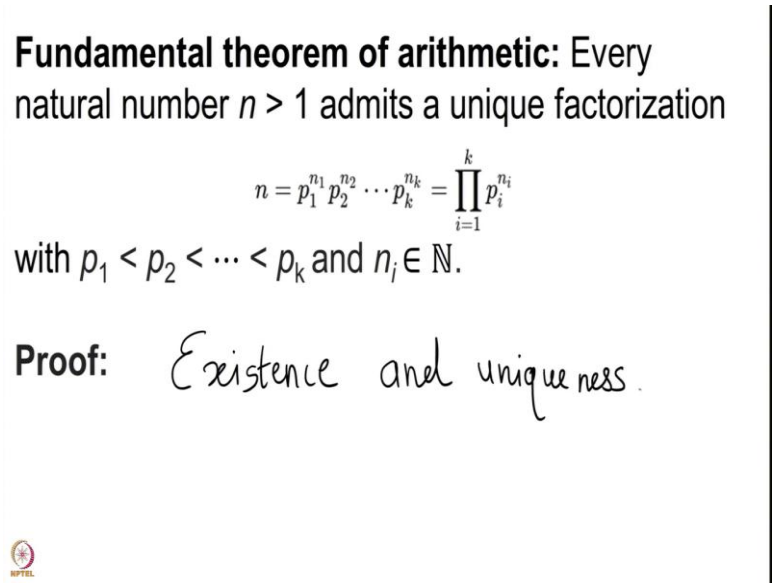
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology Bombay
Lecture 06
Fundamental theorem of arithmetic

Welcome back. I am now going to really give you the proof of the fundamental theorem of arithmetic we have been talking about it in so many of our previous lectures and only now, we are going to see a proof. The proof really required all the machinery that we have developed so far.

You will see that the previous lemma that we have proved that whenever a prime divides product of two natural numbers, then it should divide one of them, this lemma is very useful in the proof we will see that and further in the proof of the lemma itself, we use the notion of the GCD which used the notion of the division algorithm and all that, this is how typically mathematics works when you have a nice result to be proved, there is often a very nice theory that one builds up to prove this and therefore, while having the proof of the theorem as a bonus, we also several, we also have several interesting concepts, a very nice theory.

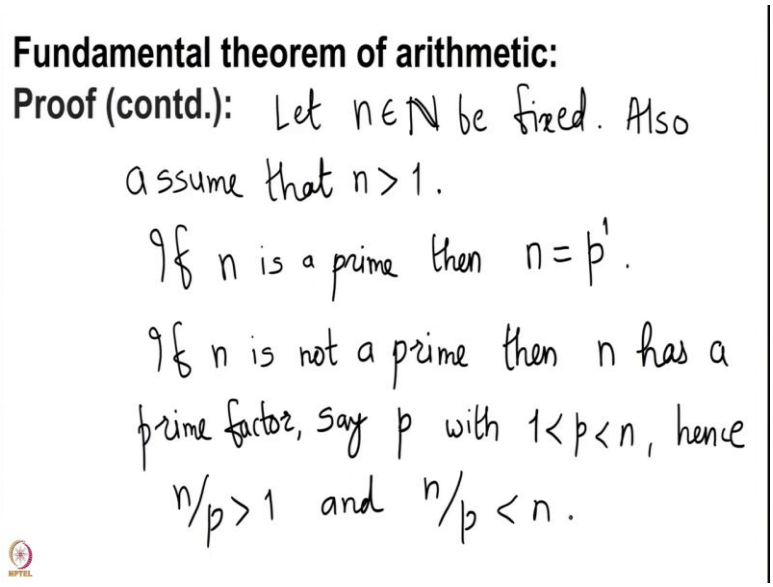
(Refer Slide Time: 1:28)



So let us begin with the statement of the fundamental theorem of arithmetic, which is here in the slide. It says every natural number n bigger than 1 admits a unique factorization n equal to p1 power n1 p2 power n2… pk power nk where you have that p1 p2 pk are put in the increasing order, these are a primes they are put in increasing orders and the powers are natural numbers. So, there are two parts that we need to prove to prove this theorem. We need

to prove existence and uniqueness. We need to prove that such a factorization exists for every natural number n and once we have proven the existence we will need to prove that the factorization which we proved to exist is unique.

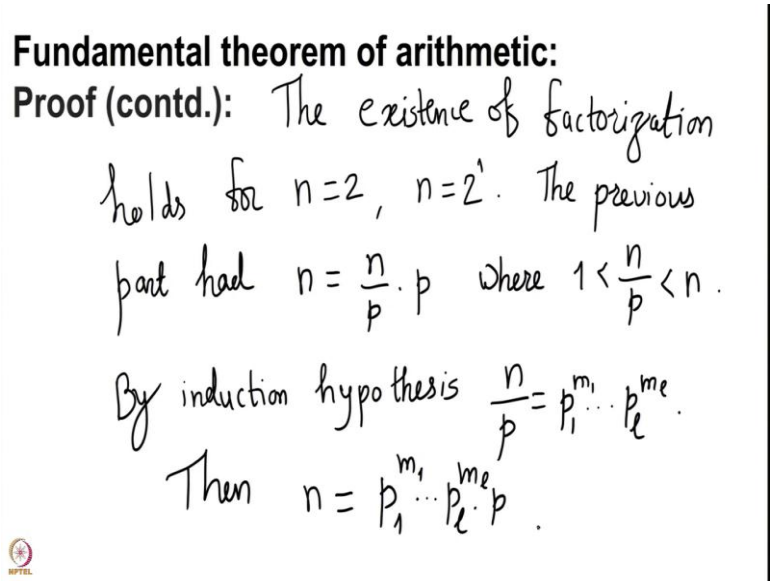
(Refer Slide Time: 2:52)



So, let us start we will use the method of induction quite liberally. So, let n in N be fixed, we fix a natural number n. Now, there are two possibilities either so, we also assume that this n is bigger than 1, so there are only two possibilities n may itself be a prime or it will have a prime factor. So, we have already seen that every integer n bigger than 1 has to have a prime factor, if n itself is not a prime it will have a non trivial prime factor of, factor of prime p which is not equal to n.

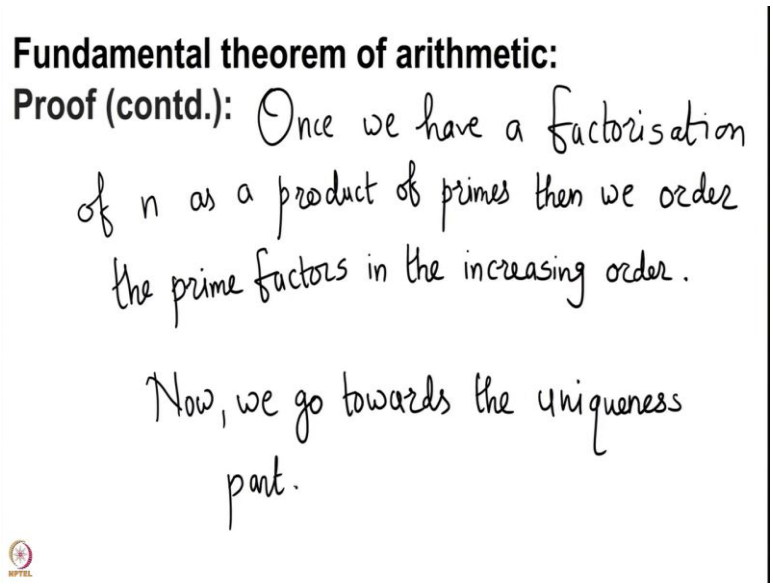
So, if n is a prime then n equal to p, disclose the existence part. If n is a prime, then we have written n as p power 1, which has proven the existence part. Let us go to the second case, if n is not a prime then n has a prime factor, say p with 1 less than p less than n, hence n by p while it is bigger than 1 because p is less than n and n by p is less than n. So we found the new natural number n by p, which is not equal to 1, it is bigger than 1, but it is strictly less than n. Here we are talking about existence of factorization.

(Refer Slide Time: 5:34)



The existence of factorization holds for n equal to 2, the existence of factorization holds for n equal to 2, where you will write n as 2 into 1 and the previous part had n as n by p into p, where this n by p is first of all bigger than 1, but is less than n, you can apply the induction hypothesis to n by p. So, by induction hypothesis n by p admits a prime factorization, and then you simply multiply by p. Then n is p1 power m1 pl power ml into p. Once we have such a factorization, you can easily arrange these primes into increasing orders. And then we are really done.

(Refer Slide Time: 7:29)



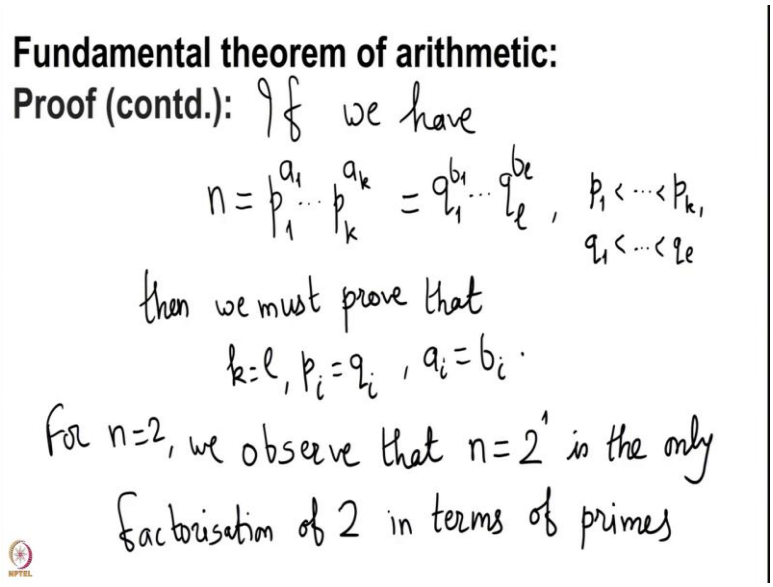
Once we have a factorization of n as a product of primes then we order the prime factors in the increasing order. So, the factorization that we wanted for n as p1 power n1, p2 power n2...

pk power nk can be easily arranged now, because we have p1 after this arrangement, we have p1 less than p2 less than… up to pk. And the powers are of course natural numbers because the powers for the n by p were natural numbers. If your prime p is a new prime, if it was not one of the p1, p2, pl then the power of p will be 1 which is a natural number. If p was one of them, then you will simply increase one of those mi by 1. So, we have a factorization as we had desired.

We now, have to go towards the uniqueness. Now, we go towards the uniqueness part. So, what do one, what does one mean to have uniqueness part we have proved that the factorization exists. That means, at least one way to write n as product of primes exists, but it can of course happen that if I do a factorization in Mumbai, I may have a factorization and if somebody else does a factorization somewhere else, then the person may get different prime factors and may altogether obtain a different factorization.

What we have to prove that such a thing cannot happen, this is what is abstract about mathematics, that a statement of the theorem, it should be true independent of the person, independent of the place, independent of the day, independent of the time, indeed independent of everything else, it should simply depend on the assumptions. The statement of the result if true should not depend on anything else. So, we now have to prove that whenever there are two such factorizations then the primes occurring in both the factorizations are the same, and then we have to prove that the powers are the same. This is what we need to prove.

(Refer Slide Time: 10:54)



If we have n as p1 power a1, pk power ak and q1 power b1, ql power bl, then we must prove we also of course assume that p1 is less than up to pk and q1 is less than upto ql, then we must prove that k is l, pi is qi and ai is bi, quite a lot to prove. We should prove that the number of primes which occurs in both the factorizations is the same, the number of primes occurring in both the factorization is the same. So, we will need to prove that k is equal to l, indeed this number can also be different.

We need to first show that these two numbers are same, then on both sides, we have the same number of primes p1 p2 pk, q1 q2 qk and we have of course ordered them in the increasing order, so we will then have that p1 is equal to q1 we will need to prove this p1 is q1, p2 is q2, so on up to pk is qk and after that we will you prove that a1 is b1, a2 is b2 upto ak equal to bk.

But we will not use all these things we will simply appeal to induction, how do we do that? So, we will need to prove the very first step of induction, which is that if n equal to 2 then there is a unique factorization. So, we observe that n equal to 2 power 1 is the only factorization of 2 in terms of primes. We observe that n equal to 2, so here we need to say for n equal to 2, for n equal to 2 we observe that n equal to 2 into 1 is the only factorization of 2 in terms of primes, maybe there is a better way to write this for n equal to 2 we observe that n equal to 2 power 1 is the only factorization of 2 in terms of primes.

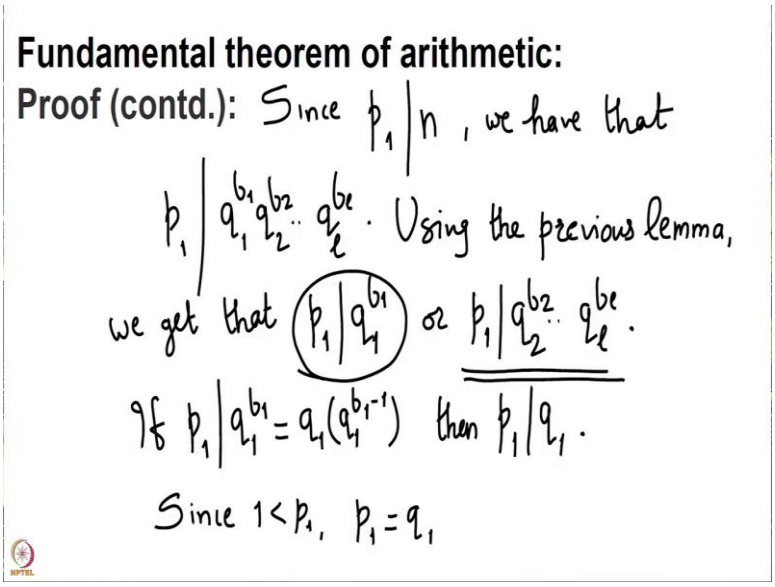
Let just think about it and let just discuss how this is the only factorization, can 2 have any other factor can 3, 5, 7, 11, 13 all the other primes can these be factors of 2? No, these are all primes which are bigger than 2, remember here we are, we are talking about a very explicit example, n equal to 2 and so, we can use all the things that we know up to now. So, we have known that whenever a divides b, a has to be less than or equal to b but the other primes are in fact odd primes and they are all bigger than 2; 3, 5, 7, 11, 13 and so on.

So, they cannot divide 2, so the only prime that can divide 2 is 2. Can it come with any other power, can it come with a power 2? No, because 2 square is 4 and then you have gone ahead, if you were able to write n which is 2 as power of 2 with any higher number, then you get a contradiction because all higher powers of 2 are bigger than 2, they cannot divide 2. Therefore, n equal to 2 has only one factorization which is n equal to 2 into 1.

So, after this we are going to use induction, remember once again that we have assumed that n equal to p1 power a1, p2 power a2, pk power ak is one factorization for n and q1 power p1,

q2 power b2, q2 power b2, ql power bl is another factorization, we want to apply induction, we have just now observed that the beginning step of the induction is done. So, once we reduce the case of n to anything smaller than n but bigger than 1, then we apply induction hypothesis to that and get our result. So, this is what we are going to do.

(Refer Slide Time: 16:29)



So, since p1 divides n, because you were able to write n as p1 into some natural number p1 divides n, we have that p1 divides q1 power b1, q2 power b2… ql power bl, so p1 divides the product of these finitely many integers. What did we prove in the lemma, in the last lecture we proved that whenever p divides, whenever p is a prime and p divides product of two natural numbers it should divide one of them. So, here I have the following thing that p, the p1 that we have started with which is a prime should divide one of the prime powers that we have here.

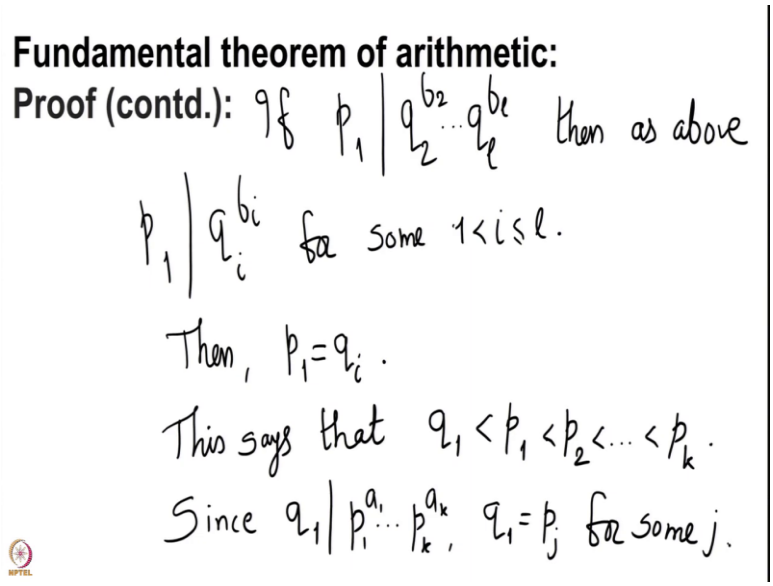
So, using the previous lemma we get that p1 divides q1 power b1 or p1 divides q2 power b2 upto ql power bl, one of these two should hold because I will write m as q1 power b1 and n as the remaining prime powers product, so p1 must divide q1 power b1 or p1 should divide the product of the remaining prime powers. In the first case, if p1 divides q1 power b1 which I will write as q1 into q1 power b1 minus 1, then p1 divides q1, in fact here we apply the lemma again to get that p1 divides q1 or it will divide q1 power b1 minus 1.

If it divides the latter, you apply the lemma again to say that p1 divides q1 or p1 divides q1 power b1 minus 2 and so on, ultimately you will reach a state where p1 must divide q1. So,

we have that p1 which is a prime, so p1 is bigger than 1 divides q1 which is another prime. Now, q1 being a prime cannot have any non trivial factors, p1 is not 1, so p1 must equal q1.

This is the conclusion that p1 is equal to q1, we started with the least prime dividing n in the first factorization, that was p1 and we started with the least prime in the second factorization, and in one case, we have proved that p1 is equal to q1. What is the case? The case is here, the case is this case, in this case we have proved that p1 must be equal to q1. Now, it is quite possible that this case occurs that p1 divides q2 power b2… ql power bl, this can also occur then, what do we do?

(Refer Slide Time: 20:37)

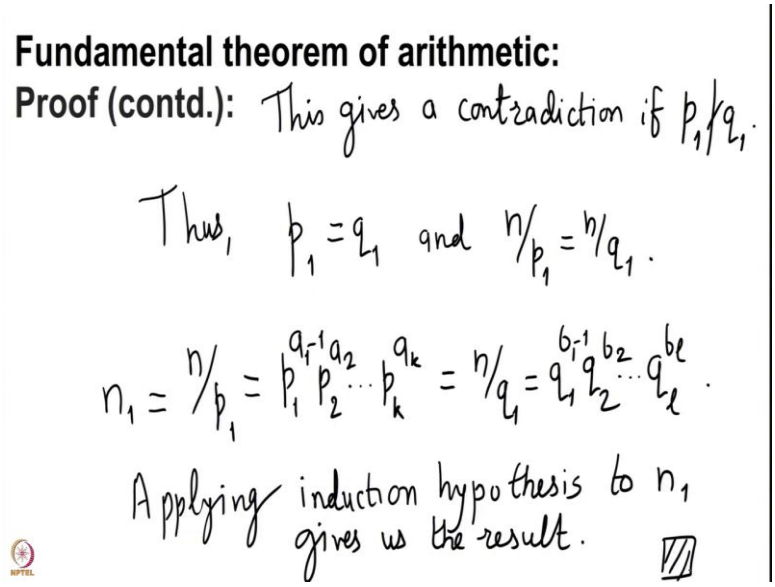


If p1 divides q2 power p2… ql power bl, then as above p1 divides qi power bi for some 1 less than i less than or equal to l, how do we see this, we will again write this product q2 power b2 up to... up to ql power bl as q2 power b2 into the remaining things. Now, p1 should divide q2 power b2 or it will divide the remaining products, if it divides the remaining products you again write it as q3 power b3 into the remaining products by doing this a finitely many times ultimately we reach that p1 must divide q2 power b2 or q3 power b3 or ql power bl all the way, it should divide one of the q power b.

But then as we have seen in the previous case again p1 will be equal to that particular qi because p1 must divide qi and p1 being a prime is bigger than 1, qi being a prime cannot have any non trivial factor, so p1 must be equal to q1, but this is a contradiction, because what we have done by taking with one prime factor in one decomposition go into the other factorization can also be done in the other way.

So, this says that, q1 is strictly less than p1 which is further strictly less than p2 and so on upto pk. Remember p1, p2, pk these were the primes occurring in the first factorization, if your p1 which is the smallest prime occurring in the first factorization happens to be equal to a qi which is 2 onwards, then q1 which is smaller than q2 has to be smaller than p1 smaller than p2 smaller than (p) and so, so on up to pk, but reversing the argument we will see. So, since q1 divides p1 power a1 up to pk power ak, q1 is pj for some j. Repeating the same argument that we have done for p1 can be done for q1 and this gives a contradiction.

(Refer Slide Time: 23:41)



This gives a contradiction if p1 is not dividing q1. So, what we have there observed? So, thus p1 is q1 and n by p1 equal to n by q1. Now n by p1, n by q1, this has a smaller factorization, we will in fact have that here we have l applying induction hypothesis, call this n1, gives us the result. So, we have indeed proved that whenever we are given any natural number it can be written as product of primes in a unique way, provided you write the factors in the increasing order.

Once again, let me quickly in very brief go over the proof. There were two parts of the proof existence and uniqueness. The existence theorem part was proved by appealing to induction, so was the uniqueness part done. So, what is the beginning step of the induction? We observed that 2 has a prime factor decomposition, which is 2 equal to 2 into 1. And later we also observed that this decomposition is the unique decomposition for 2 as prime product of primes.

Now, we will go to a general n, if the n was a prime, you would already have a factorization n equal to p. If n is not a prime, then you would look at n by p, which we call n1 induction hypothesis gives you a factorization for n1 multiplying that factorization by p gives you a factorization for n. So the existence of factorization is proved using the induction in this way.

Now, we want to prove the uniqueness. So, for the uniqueness we assume that there are two factorizations p1 up to pk power a1 up to ak, q1 upto ql power b1 upto bl, then we start with the smallest prime dividing n on the left hand side factorization, we prove that it has to be equal to one of the primes on the other side. And since this can be done on both sides, we must have that the smallest one p1 has to be equal to the smallest one q1, since they are same cancel them out you get n1, which will have a reduce, which will have a smaller factorization.

Appeal to the induction hypothesis to get that k equal to l, ai equal to bi and pi equal to qi and therefore, we have the proof of uniqueness using the induction method. Induction method is a very powerful method and we have seen one very good application of the method. So the fundamental theorem of arithmetic is proved. In the next lecture, we will see some comments about primes. And then we will go to the theory of congruence, which is going to be the next part of our course. Thank you and I hope to see you again.