A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 21
Wilson's Theorem

Welcome back. In our last lecture we have done a very intricate analysis of computing the number of the square roots of 1 in z mod and z. It was first of all factoring n into several prime powers and then solving the equation x square equal to 1 modulo these prime powers. That gave us linear congruences mod each of these prime powers. And then we got a set of systems of simultaneous linear congruences which have unique solution modulo the product of all those moduli which is your n and that is by Chinese remainder theorem.

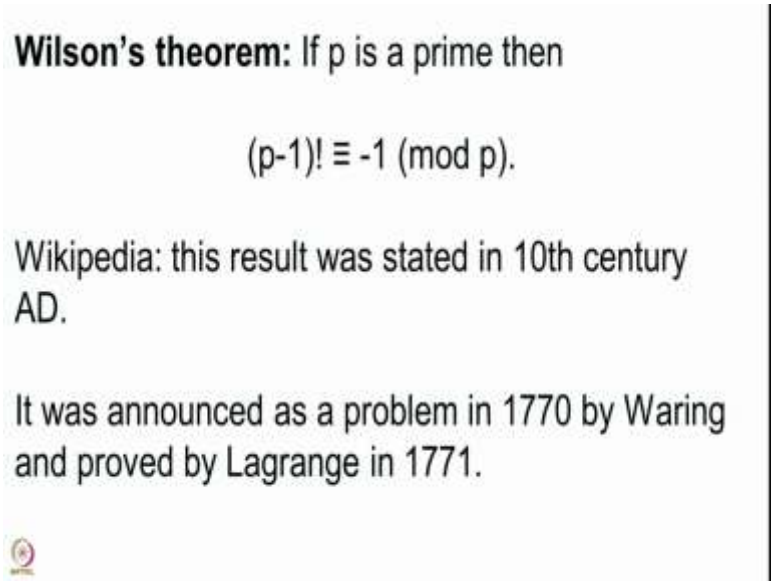
And so we can compute the exact number of solutions to x square congruent to 1 modulo n. I would suggest that you take n equal to some number like 30 or say 48 and actually work out all those things quickly and that will tell you how that intricate analysis works in some very particular cases. Now, we are going to take our attention to somewhat different type of mathematics.

In number theory, there is a function called the factorial function. This is one symbol that is lifted from literature which is the symbol of the exclamation mark and we use it to denote the factorial. So a factorial is 1 into 2 into 3 into dot, dot, dot all the way up to a that is our factorial function. It is a expanding function as a goes to infinity, a factorial goes to infinity much faster than any polynomial in a.

However, when you look at d z by n z, or in particular the z by p z, the factorial function is not going to increase because when you look at z mod n z, you take powers or you take products. You are allowed to take the multiples of n out. You after all have only finitely many elements in z mod n z. You have exactly n elements in z by n z, starting from 1 to n or if you want to start from 0 then you go up to n minus 1.

So it is interesting to ask what would happen when you take the factorial function in such a ray. And this is a very interesting result that we now have. This is called Wilson's Theorem.

(Refer Slide Time: 02:58)



So the theorem says, that when you talk a prime p and you take p minus 1 factorial, so that means you take the set z mod p z, remove 0. So you have all the non-zero elements there 1, 2, 3 up to p minus 1. If you include p, that p is 0, so we are not going to include that back. So you have only the non-zero elements 1, 2, 3 up to p minus 1, p minus 1 factorial is the product of all these numbers.

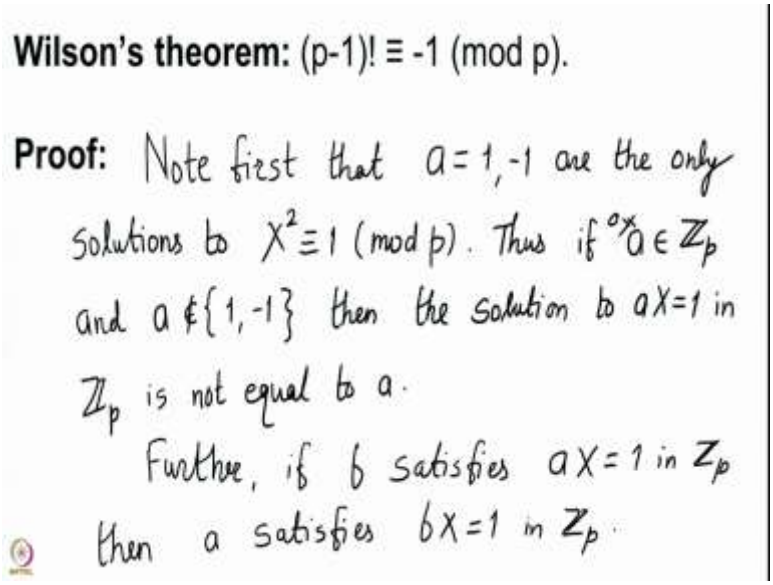
And it is interesting to note that this is equal to minus 1 when you are working in the set z mod p z. Now, this very important and very basic theorem is given the name of this mathematician John Wilson, but as it happens often in mathematics or in several branches of science, this is not originally due to Wilson, in fact it is not at all due to Wilson. This was stated in tenth century AD. John Wilson is a mathematician from 18^{th} century this was known in 10^{th} century AD.

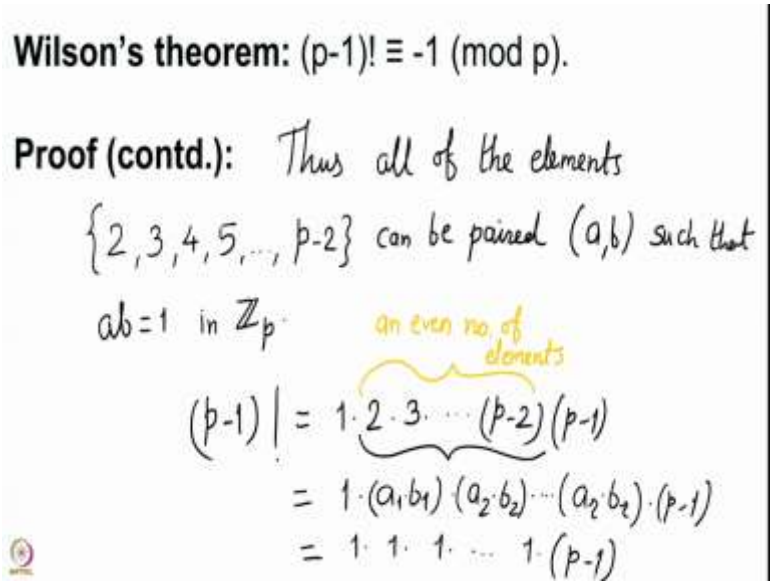
And in fact Wilson did not solve this at all. Wilson's teacher Edward Wearing, he gave this as a problem. He computed this p minus 1 factorial for several primes and he noticed that this is congruent to minus 1 mod p. So as it is very common with teachers, Edward Wearing gave it as a problem to John Wilson to show p minus 1 factorial is congruent to minus 1 modulo p for every prime.

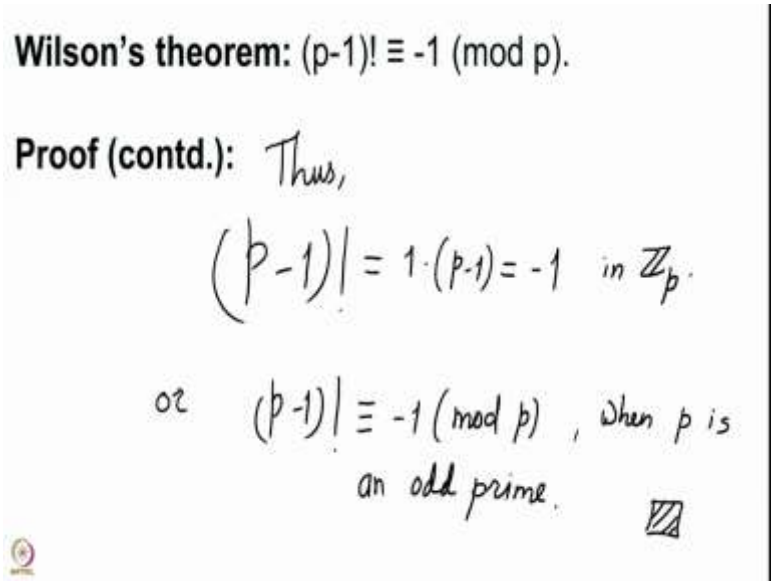
But Wilson could not do it. However it was Lagrange who did it in the next year 1771. But since it was Wilson who made it well known, who posed this as a problem when he received it from

Edward Wearing, and because he could not solve he asked people, and so it came to be known as Wilson's Theorem. The proof of this is very easy and it will draw upon the thing that we have done earlier, that the square roots of 1 in z mod p z when p is prime are only 1 and minus 1. Remember those calculations or remember that result. That is a result that we are going to use here.

(Refer Slide Time: 05:30)







So we go towards proving this statement that p minus 1 factorial is congruent to minus 1 modulo p. So note first, that a equal to 1 and minus 1 are the only solutions to a square, or we should perhaps say x square congruent to 1 mod p. So what it means to say is the following, thus if you have a from this z p, or z p and you take a to be different from 1 and minus 1, then the solution to a x equal to 1 is z p has or the solution to a x equal to 1 in z p is not equal to a.

Let us think about this statement again. We start with a non-zero element in z p. So we are looking at elements 1, 2, 3, 4 all the way up to p minus 1. We fix 1 a from this set and we pose this question, what is the solution to ax equal to 1. Now this is same thing as solving a x congruent to 1 mod p, and since you have taken p from 1 and p minus 1, the GCD of a and p is 1. Therefore you have one solution and you actually have a unique solution.

The only question we are interested in is whether this solution can be equal to a itself. We know that a x equal to 1 has a solution. So we know that there is an element b again in z p such that a into b gives you 1. This is something that we have done quite often, you know, when we looked at a equal to 5, let us say and p equal to 7, and we wanted to solve for 5 x congruent to 1 modulo 7. This had occurred it one of the solutions of linear equations, linear congruences or while solving the simultaneous systems of these.

And we observed that 5 into 3 is 15 and 15 is congruent to 1 mod 7. So the equation 5x equal to 1 in z7 has solution 3, which is different from 5. However if you were looking for 6x equal to 1

modulo 7, 6 is itself the solution. And the reason for that is 6 is equal to minus 1. If you were looking for solutions to x equal to 1 modulo p, x equal to 1 is the solution. So when your coefficient a happens to be 1 or minus 1, that a is the only solution.

But the previous analysis of (solve) looking for solutions of x square equal to 1 modulo p, when p is odd prime told us that there are no other solutions. So a x equal to 1 whenever a is different from 1 and minus 1, whenever there is a solution, you will have that the solution is different from a. This is one thing that we keep in mind. There is another thing that we should remember.

Further if b satisfies a x equal to 1 in z p, then a satisfies b x equal to 1 in z p. So you have, earlier we have seen that a x equal to 1 has a solution other than a. Call that solution to be b. Then you can ask the same question for b. So you have b x equal to 1, this is another solution that you have created. That has solution to be the earlier a.

So going back to our example we had 5x equal to 1 in z7, we noted that 3 was the solution. Then you ask, if you ask for 3x equal to 1 in z 7, 5 will be the solution. So all the numbers from 1 to p minus 1, other than 1 and minus 1, can be put in pairs, were a will be put up with b, where the property of a and b is that a into b is equal to 1 modulo z p. This is what we are going to do.

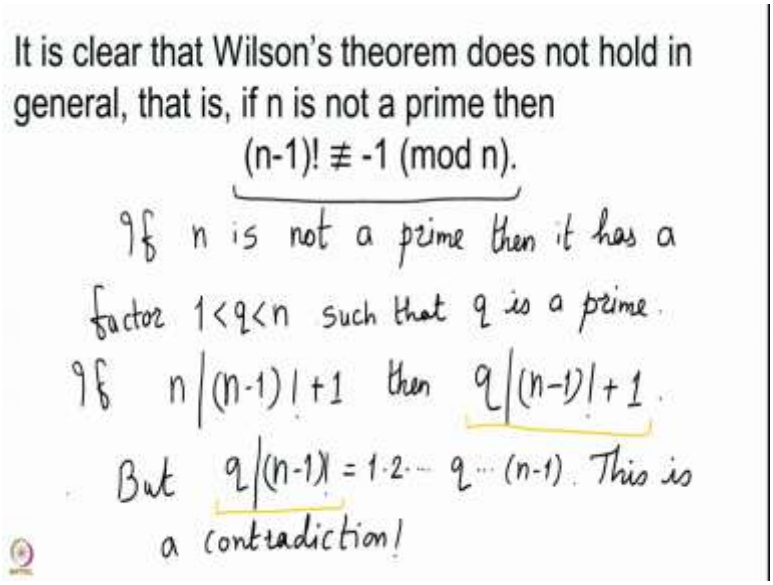
Thus all of the elements, I will not take 2, I will not take 1 so I will start with 2, 3, 4, 5 up to p minus 2 can be paired a b such that a b equal to 1 in z p, or a b congruent to 1 modulo p. So when I take the product, p minus 1 factorial, this is 1 into 2 into 3 and so on up to p minus 2 into p minus 1.

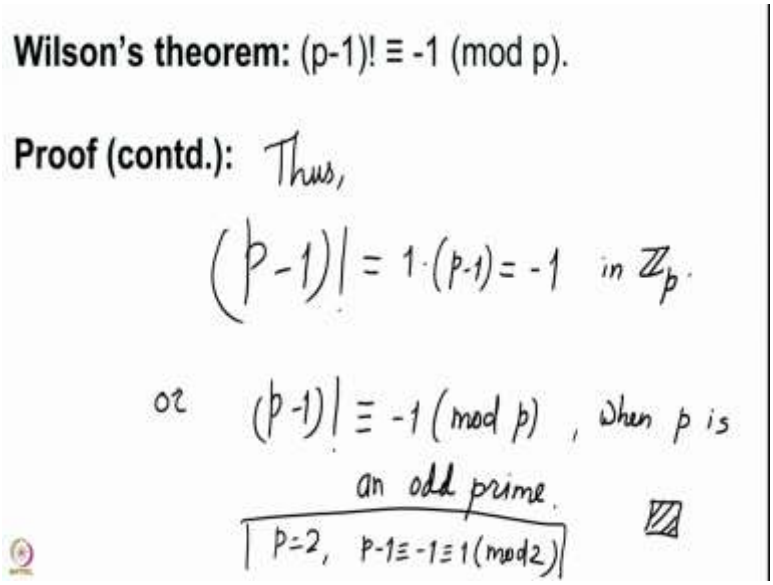
So these elements have been paired as a1 into b1, where a1 and b1 have the property that their product is 1 in z p. a2, b2, so on up to ar, br. Remember this is an even set, an even number of elements. This is because your p is odd, so 1 up to p minus 1 are even elements and you have removed two namely 1 and p minus 1 from them, so what you get is an even number of elements and therefore they can be easily paired. And finally we have this last element p minus 1.

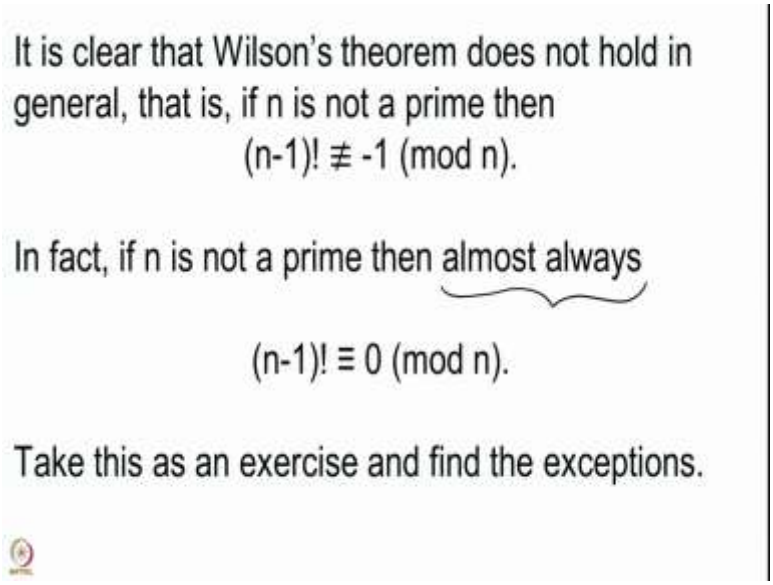
Note that all these products are 1, and finally we are left with p minus 1. Now we are almost there. Thus, p minus 1 factorial equal to 1 into p minus 1 which is really minus 1 in the set z p, or what we have is p minus 1 factorial is congruent to minus 1 mod p, when p is an odd prime. So

the proof is quite simple but remember that the intricate analysis that we have done for the number of x square equal to 1 modulo n is one of the major steps behind the simplicity of this product. Alright, so we have such a nice result, and you may ask, what would happen in general?

(Refer Slide Time: 14:48)







So clearly, Wilson's Theorem does not hold in general. In fact, what that means is that if you take number n which is not a prime, you may ask, you know earlier slide said that p is odd, if you put p equal to 2, then yes, that also holds, p equal to 2. Here p minus 1 is minus 1, but that is also 1 modulo 2. So there is actually no statement for p equal to 2. But we may say that p minus 1 factorial congruent to minus 1 holds for all primes, that is something that we can say.

And when we ask for the same question, whether it holds in general, we are asking for a number which is not a prime. You may look for n equal to 4. And you will see that n minus 1 factorial which in the case of n equal to 4 is 3 factorial, 3 factorial is even number, so clearly it cannot be minus 1 modulo 4. So you already have that whenever n is nt a prime, that n is a composite number and then the smallest composite number 4 gives you that the equation does not hold.

In fact, you can say more, we will say, so if n is not prime, if n is not a prime, then it has a factor which is not equal to 1 and not equal to n by the very definition of primes. But you can also get that factor to be itself a prime, right? So when you have this factor, and if you have that n divides n minus 1 factorial plus 1, which is to say that this equation holds instead of not holding, then q divides this because q divides n.

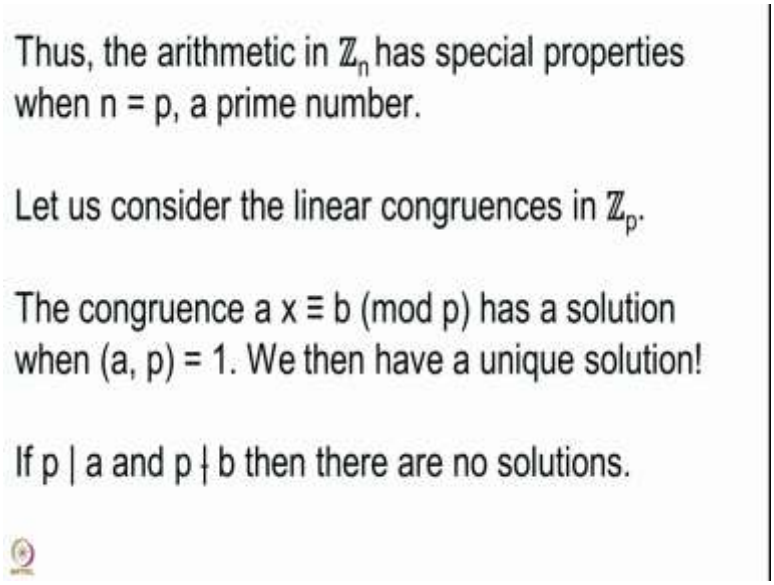
But q is less than n, so q is less than or equal to n minus 1. So you have that q also divides n minus 1 factorial. This will be 1 into 2 into dot, dot, dot somewhere q will have to appear and then you go up to n minus 1. And this is a contradiction. You have that q divides n minus 1

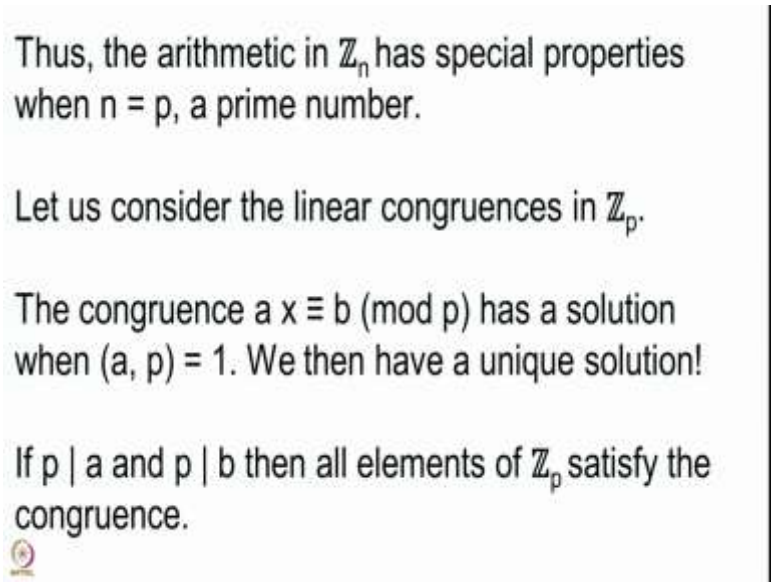
factorial and also that q divides n minus 1 factorial plus 1 that cannot happen. So on one hand you have this, on the other hand you have this, which is not possible.

So, clearly whenever n is not a prime, we do not have Wilson's Theorem. But in fact something more can be said. In fact if you have that n is not a prime, then almost always we have will have that n minus 1 factorial is 0 mod n, n will divide n minus 1 factorial. This is something that always holds except one or two exceptions. So, I will what, I will now give this to you and as an exercise I will not give you the solution, neither will I give you any hint to solve this problem.

Take this as an exercise and find the exceptions, by exceptions I mean the situations where you do not have it to be 0 mod n. So almost always is not the same as always. Almost always means except for a few cases you have this. So those few cases where n is a composite number but n minus 1 factorial is not divisible by n, those are the composite, those are the cases that I want you to find. And in the remaining cases, I want you to prove that n minus 1 factorial is congruent to 0 mod n.

(Refer Slide Time: 19:25)





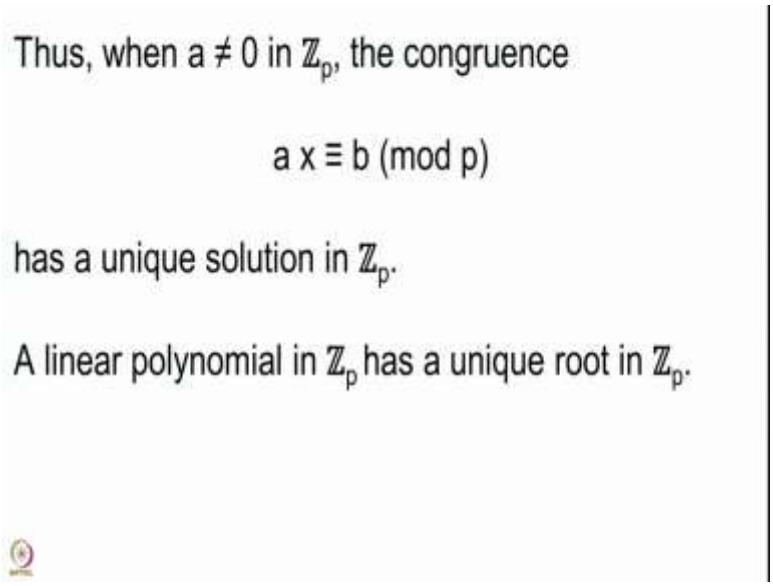
So this tells us that there is something very special which happens when n is a prime number. The arithmetic in z p has some special properties compared to the arithmetic in a general z n. So what does it mean? Let us go through these things once again. If you are looking at linear congruences modulo a prime number, then we see that the congruence a x congruent to b mod p has a solution, when a comma p is 1.

Now p has the property that when you look at z p, only the 0 is the one which does not have GCD equal to 1 with p. All other numbers have GCD equal to 1 with p and therefore a x equal

to b mod p will have solution whenever a is not 0 in z p. If you have p dividing a but p and ofcourse when because the GCD is 1 we have a unique solution. Further if you have p dividing a but p does not divide b, then there are no solutions. So you will have 0 x equal to a non-zero b congruent to p cannot give you a solution.

If you have that p divides a and p divides p, then everything is the solution, because this is like asking for 0 x equal to 0 mod p. And whenever you put anything for x, you are going to get the answer to be 0. So barring the cases where p divides a, the interesting cases are where p does not divide a, or when you are looking at the elements in z p, you are looking at the case where a is not equal to 0.

(Refer Slide Time: 21:20)



Whenever a is not equal to 0, the congruence a x equal to b has a unique solution. This is something which happens for complex numbers. This is something which happens for real numbers, this is something which happens for rational numbers also.

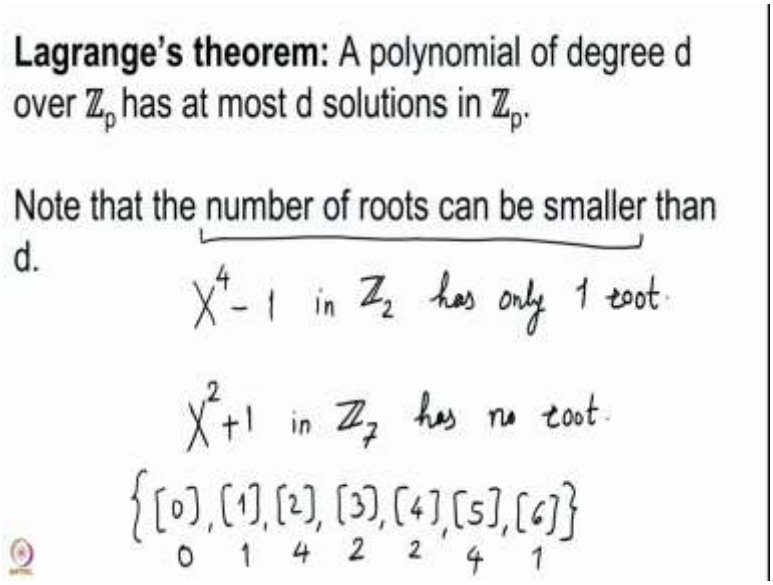
So whenever you have any complex number a and a complex number b, and you ask for a x equal to b, if the complex number a is not 0, you can simply invert that ad you have the solution x equal to b upon a, or x equal to b into a inverse, or a inverse into b, the multiplication is commutative.

Then we would say, alright, for z p, there are things which are happening like the complex numbers or real numbers. But for complex numbers and real numbers you have one more interesting thing. That is, when you have a degree d polynomial, any such polynomial will have at most d roots. This is something that we have again used. This is called the Fundamental Theorem of Algebra.

It says that if you are looking at a polynomial in degree d in one variable over complex numbers, it has exactly d roots. If you are looking at a polynomial over r, you may have a smaller number of roots, because some of these roots will actually be in c, they will not show up when you look at only r. So for r, or for q, the rational numbers, the correct statement of the theorem says that, a polynomial in degree d has at most d roots.

You may have a smaller number of roots or you may have it to be equal to d, but you will never have it to be more than d. The condition is that the polynomial should be a degree d polynomial. Does the similar theorem hold for z p? That is the question and yes, it does hold for z p.

(Refer Slide Time: 23:22)



And this theorem is theorem due to Lagrange. You will see that Lagrange has done quite a bit of fundamental work in number theory among other areas of mathematics. And this is also a theorem due to him. So her says that if you start with a polynomial of degree d over z p, over z p means that you have coefficients coming from z p, that is what it means.

Then any such polynomial has at most d solutions in z p. Before we go to the proof, we wonder what would happen when you have other cases, or is there anything that we need to be careful about. So number one, note that that number of roots can be smaller than d.

So there are indeed examples where the number of roots can be smaller than d. For instance, if you are looking at x raise to 4 congruent to 1, or to say it in other words, if you are looking at the polynomial x square, x to the 4 minus 1 in let us say z 2, this has only one root, namely x equal to 1. But here you may say that z 2 actually has only two elements 0 and 1. 0 to the 4 is 0. And 1 to the 4 is 1.

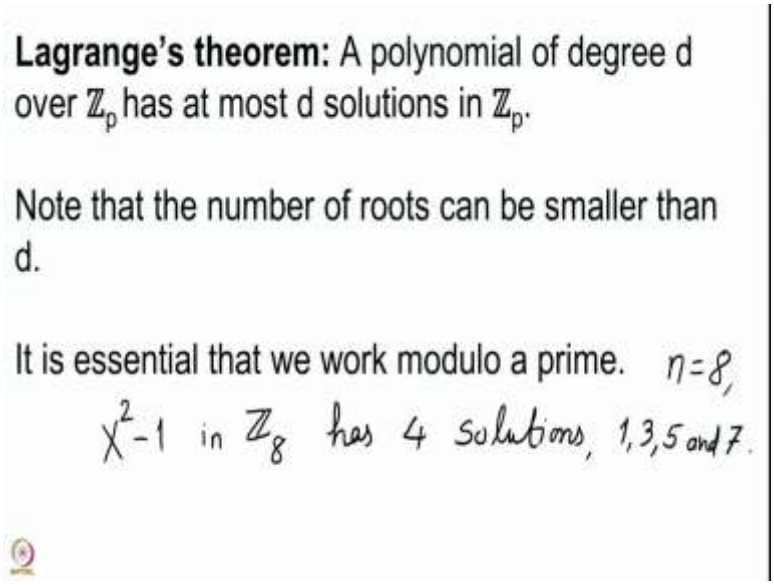
So that the fact that there are smaller than 4 roots, you have only one root which is smaller than 4, is not very striking because z 2 alone has elements which are smaller than 4. So if you are looking at a polynomial of degree d, which is the degree being bigger than p, then it should not be surprising that you have the number of roots to be smaller than p.

So if I give you an example, I should give you an example where the prime p is bigger than the degree and yet we have smaller number of roots. And so we will look at x square plus 1 in let us say in z 7 has no root. So x square plus 1 in z 7 has no roots. You can actually quite quickly check this. You have 0, 1, 2, 3, 4, 5 and 6. And let us just compute their squares.

So 0 square is 0, 1 square is 1, 2 square is 4, 3 square is 9 which is 2. And 4 is minus 3, so its square is 2, 5 is minus 2 so its square is 4 and 6 is minus 1 so its square is 1. So there is no solution to x square plus 1, x square plus 1 is same as x square minus 6 when you are looking at z 7. So there are no solutions at all. Your degree of the equation is 2.

Your number of elements is z 7 is 7. You could have had two solutions, one solution. But this solution, this equation has no solution. So this is indeed an instance where the number of roots is smaller than the degree d.

(Refer Slide Time: 26:56)



What if we work with something which is not a prime? Does this result still count? Does this result still hold? No. It is important that you work modulo a prime. If you take n equal to 8 and we have solved the equation x square congruent to 1 mod 8, so x square minus 1 in z 8 has four solutions. 1, 3, 5 and 7. You have four solutions which is bigger than the degree.

So indeed it is very much important that you work modulo a prime. If you work modulo a composite number then Lagrange's theorem need not hold. We will see a very simple proof of Lagrange's theorem in the next lecture. And then we will do some more analysis with the set z p. So I hope to see you again in the next lecture. Thank you very much.