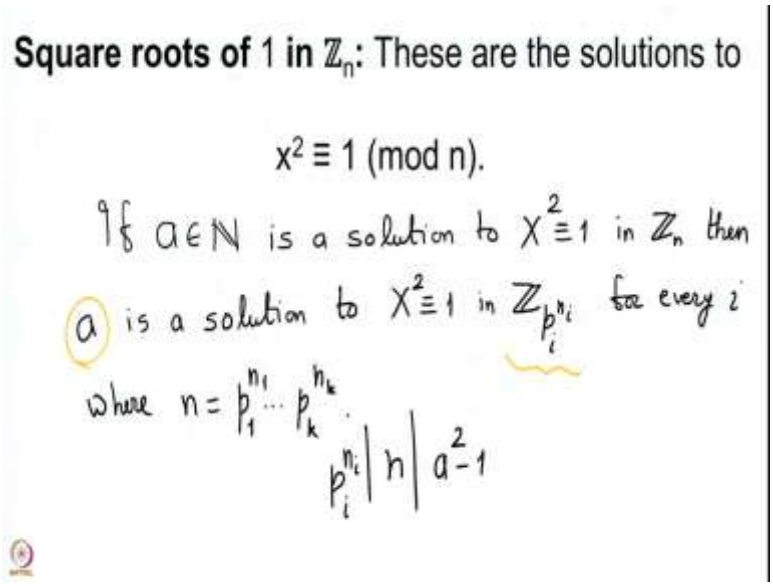
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 20
Using the CRT, square roots of 1 in Zn

Welcome back we have proved the one of the most important theorems in Number Theory, the Chinese remainder theorem. And there in the last lecture we also took some problems related to the theorem. We applied the theorem in various cases, we are going to see one more application of this theorem and do some more computations in the set Z modulo nZ.

So, this is the set which we denote by Z sub n and we will call it Zn or sometimes we call it Z n. The set of integer Z is sometimes pronounced as Z. So, Zn is the set that we will be looking at and we will start some arithmetic in it. So, we have solved linear congruences in Zn, we saw exactly when a is congruent to b mod n has solutions. We go one step further and we try to solve quadratic congruences.

So, the very beginning step is to solve for x square congruent to 1 modulo n. This is the non-linear the quadratic congruence that we are going to solve. In general it is not easy to give the solutions to the equation x square equal to 1 in Zn. But what we can definitely do is to compute the number of solutions.

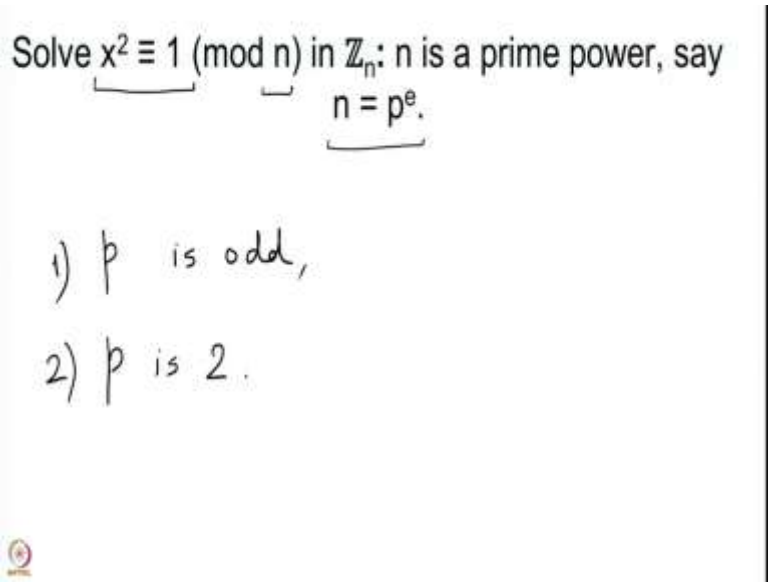
(Refer Slide Time: 01:49)



So, what we want to do to begin with is to compute the number of solutions to x square congruent to 1 mod n. These are the square roots of 1 in Zn, the square roots of the identity element in the set Zn. We noticed one thing immediately that whenever we have some natural number a, so if a in the set of natural numbers is a solution to x square congruent to 1 in Zn, then a is a solution to the same equation. But we are going to change the modulus.

So, instead of looking at Zn, we are going to look at Z pi power ni for every i, where we have that n is p1 power n1, pk power nk. So, whenever we have n dividing a square minus 1, we have these pi power ni, also divide a square minus 1 and therefore we get that the number a is a solution modulo pi power ni also. Therefore to solve the equation x square congruent to 1 mod n, we should first solve it modulo the prime powers.

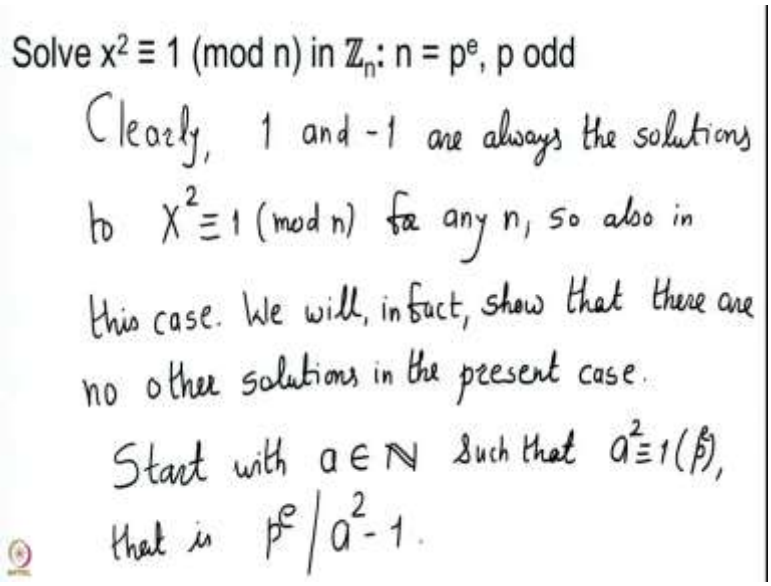
(Refer Slide Time: 03:50)



So, we are going to solve the equation x square congruent to 1 mod n, modulo n, where n is a prime power, this is what we are going to do. But then there are two cases, case 1 is where our prime is odd and case 2 is when p is the oddest of all the primes, which is that p is equal to 2, these are the two cases, that we are going to study.

So, case number 1 once again is where we are solving x square congruent 1 modulo power of an odd prime. And case number 2 would be where we will solve for x square congruent to 1 modulo 2 power e, those are the two cases and then we will combine these two cases and come back to our general equation x square congruent to 1 modulo n, and we will see how many solutions there can be.

(Refer Slide Time: 05:01)

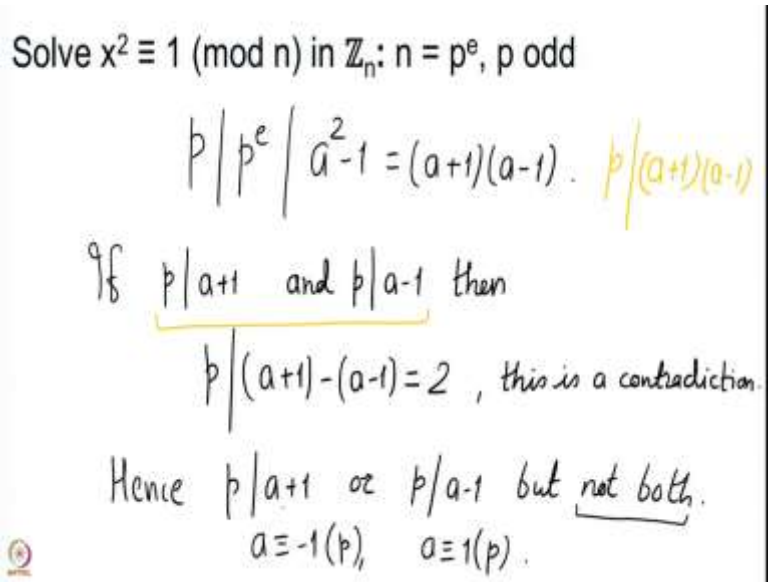


So, we begin with p equal to an odd prime, this is what we have x square congruent to 1 mod n in Zn, where n is p power e, and p is odd. So, there is one thing that everyone should notice immediately, which is that there are two God-given solutions 1 and minus 1 are always the solutions to x square congruent to 1 mod n for any n and so also for p power e, we will have these solutions.

So, also in this case, but we will actually show that there are no further solutions. We will in fact show that there are no other solutions in the present case. So, when p is an odd prime and we are looking at Z modulo n, where n is power of this odd prime, then we will show that x square congruent to 1 mod n has only two solutions and those are the a equal to 1 and a equal to minus 1.

So, suppose a in natural number is a solution, we will then prove that a has to be congruent to 1 mod p, or that a has to be congruent to minus 1 mod p, this is what we will show. So, start with a solution a such that a square congruent to 1 modulo p and by this we mean that here it is p power e, p power e divides a square minus 1, this is what we have, whenever you have a square congruent to 1 modulo a number you will have that the number n divides the difference of the numbers which are there on the two sides of the congruence side.

(Refer Slide Time: 8:08)



Now, it is a high school mathematics to see that the a square minus 1 is product of a plus 1 and a minus 1. So, what we ultimately get is that p divides this product, so we get that p divides a plus 1 into a minus 1, this is what we get but P is a prime and whenever a prime divides product of two numbers, it will have to divide one of the two.

So, here we have three cases it will either divide only a plus 1 and not divide a minus1, or it will divide only a minus 1 and not divide a plus 1, or it will divide both a plus 1 and a minus 1. These are the 3 possibilities, however if p divides a plus 1 and p divides a minus 1 then we will have to divide the difference which is a plus 1 minus a minus 1, as you see this difference is 2, a will get cancelled 1 minus-minus become plus, 1 plus 1 is 2, but this is a contradiction.

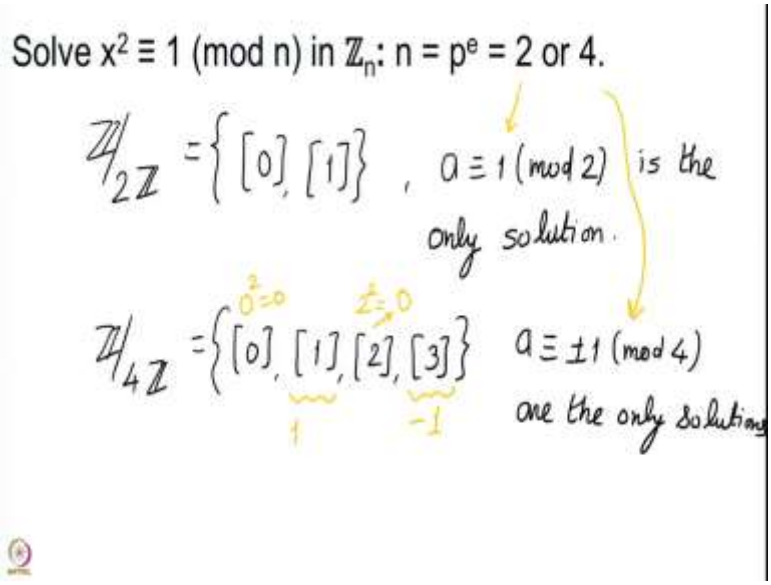
Because p is an odd prime, p being a prime when it divides 2, it will have to be equal to 2, but p is odd and 2 is even. So this contradiction says that the initial assumption that we had that p divides both a plus 1 and a minus 1 cannot hold. So, p will divide exactly one of them, it divides both, it divides the product of them and if it divides both then we have a contradiction.

Hence p divides a plus 1, or p divides a minus 1, but not both and this already tells us that the first case is that a is congruent to minus 1 modulo p, and the second case says that a is congruent to one modulo p. So, there are precisely two cases in the case of p being an odd prime that the solutions to x square congruent to 1 in where p power e will have to be just 1, or minus 1.

So, this is what we have done here is for p, but the case that it cannot divide both will tell you that when p divides a plus 1 all the powers of p, which are p power e will have to divide a plus 1, they cannot divide a minus 1. So, we actually get that, we have the possibility modulo p power e also to be only that a is 1 mod p power e, or is a is minus 1 modulo p power e.

So, to summarize whenever p is an odd prime in the set Z mod p power e Z, there are only two solutions to x square congruent to 1 mod p power e and those are a equal to 1 modulo p power e and a equal to minus 1 modulo p power e, for all odd primes the situation is the same. When we go to the even prime p equal to 2, there the situation is somewhat different.

(Refer Slide Time: 12:28)



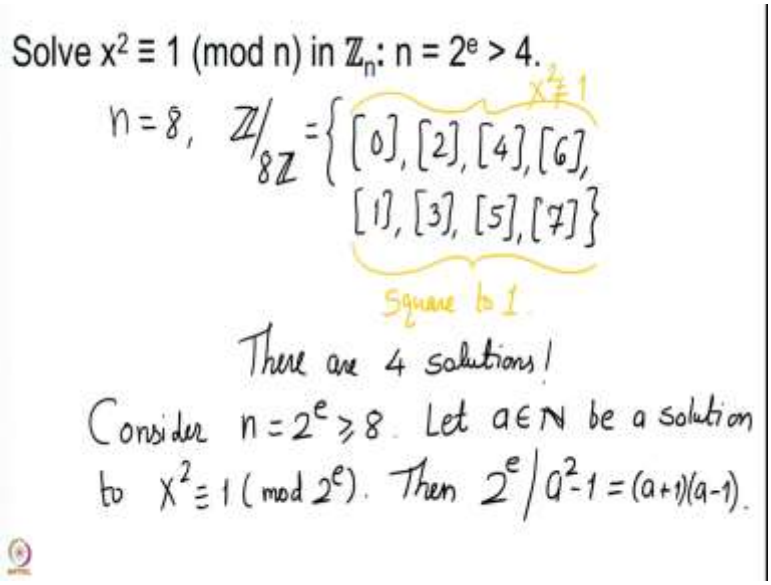
We do the case of p power e equal to 2, and p power e equal to 4 separately and then come 8 onwards we will be dealing the case differently. So, let us just look at these sets, let us write them down. So, here we have this set to be 0 and 1, 0 square is 0, 1 square is 1. So, 1 or what we would say as a congruent to 1 mod 2 is the only solution, remember I had said that minus 1 and 1 are always the solutions. But unfortunately modulo 2 1 and minus 1 happen to be congruent to each other.

So, these two which were distinct elements in Z mod an Z, they collapse to a single element, when n is 2. And therefore here we have this as the only solution. Let us go to the next set which

is Z Mod 4 Z, we have 4 elements 0, 1, 2, and 3 as we know that a congruent to 1 mod 4 and a congruent to minus 1 mod 4 these are always the solutions.

So, what is 1 mod 4? That is simply one the class of 1, this is 1 mode 4 and this is minus 1 mod 4, these two are always the solutions. And so they are solutions here also, if you take the square of 2 you get 0, 2 square is 0 and ofcourse 0 square is 0. So, it tells you that in Z mod 4 Z. Now, there are two solutions, so for p power e equal to 2, we have one solution. So, this gives you one solution and this gives you that there are two solutions, for p power e equal to 8 and onwards situation is going to be different.

(Refer Slide Time: 15:15)



So, we begin with the case where n is 8 and let us write this set carefully, we have 0, we have 2, we have 4, and 6, I am writing all the even classes first, then I write the odd classes and note here that all these numbers they square to 1, the squares of all these four numbers is 1, 1 square is ofcourse 1 and 7 square, so remember 7 is minus 1 when you are looking at modulo 8,1 square is 1 and 7 square which is also minus 1 square that is 1.

But these two middle numbers 3 and 5 their square 3 square is 9, which is 1 modulo 8 and 5 square is 25 which is also 1 module 8. So, here we have 4 solutions ofcourse these numbers do not square to 1. So, their square is not 1, so what we get ultimately in the case Z mod 8 Z, that there are 4 solutions this is a very striking situation, this is completely different from what we

have seen so far, we saw that modulo a prime power there are exactly two solutions 1 and minus 1, modulo 4 there are two solutions 1 and minus 1 and modulo 2 there is a single solution.

So, other than 1 and minus 1 which happens to collapse in the case of n equal to 2, we have not seen any different solution. But when we go to 8 the prime power becomes 8, we have 4 solutions. What will happen when you go to 16? Let us just think about it for 16 we have 1 square which is 1, and 15 square which is 225 which is 1 module 4, if you do not say it quickly remember that 15 is minus 1 modular 16, therefore its square is going to be 1 module 16.

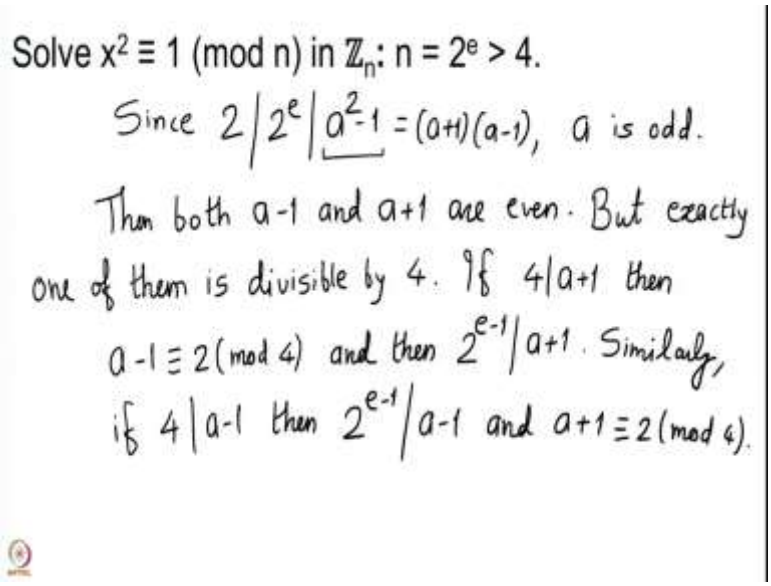
But there are two more numbers, the number 7 its square is 7 square is 49 that minus 1 48 is divisible by 16, and similarly 9 square is 81 when you subtract 1 from 81 you get 80 that is also divisible by 16. So, we have four square roots of 1 modulo 16. 1, 7, minus 7, minus 1, are there any more? That would be the natural question and we will prove that there are no further.

Whenever you have n equal to a power of 2 which is bigger than or equal to 8, then there are exactly for solutions to x square congruent to 1 modulo n. This is the thing that we would now like to prove. So, consider n equal to 2 power e and assumed that this is bigger than or equal to 8, let a in the natural numbers be a solution to x square congruent to 1 mod this 2 power e.

Then ofcourse 2 power e divides a square minus 1 and we recall our high school mathematics once again to write it as a plus 1 a minus 1, we have done exactly what we had done in the prime power case. But now there is a different thing, here 2 power e divides a product of two numbers. So, in particular 2 divides the product of these two numbers.

But if 2 divides the product of these two numbers 2 will have to divide one of them, it may divide a plus 1, it may divide a minus 1 and as we know the third case that it may divide both, in this case in contrast it has to divide both, the first two cases that 2 divides only a plus 1 and not a minus 1 or 2 divides only a minus 1 and not a plus 1 is not going to occur. How does that happen?

(Refer Slide Time: 20:32)



Since 2 divides 2 power e, which divides a square minus 1, which we will further write as a plus 1 a minus 1, a is odd, because 2 divide a square minus a square minus 1. So, a square minus 1 is an even integer, so a square is an odd integer and then a has to be odd, if a was even a square would be even and then a square minus 1 would be odd, which would be a contradiction.

So, here a is odd and then both a minus 1 and a plus 1 are even and therefore 2 has to divide both of them, 2 will divide a minus 1 and 2 will also divide a plus 1. So, when we have to decide modulo 2 power e, we know that the factors that copies of two that are there in 2 power e, one of them has to go and divide a minus 1, one another copy has to go and divide a plus 1, what about the remaining ones, will they also split?

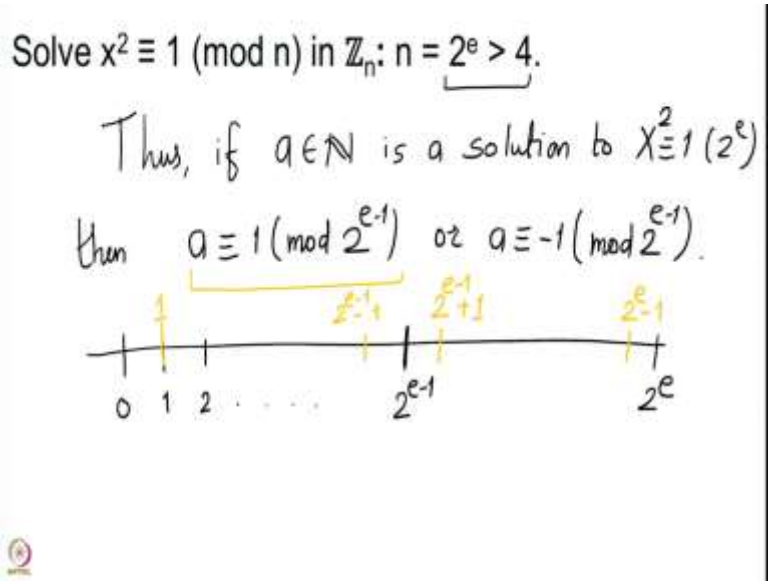
Will some of them go and divide 1, will the remaining ones go and divide the other, or do they all go to one of those two factors? That is the thing that we now have to think about. But then we see that a minus 1 and a plus 1, these are both even. So they are both 0 modulo 2, but their difference is only 2. So, one of them when you go modulo 4, one of them will have to be 0 mod 4 and the other will have to be 2 mod 4.

But exactly one of them is divisible by 4 both cannot be divisible by 4, because then 4 will have to divide the difference which is 2. So, exactly one of them is divisible by 4, if you assume that 4 divides a plus 1 then a plus 1 is 0 mod 4 and therefore a minus 1 is 2 mod 4 and then all the

remaining powers of 2 will necessarily divide a plus 1 because no higher power of 2 other than 2 can divide a minus 1, a minus 1 is just 2 mod 4, even 4 does not divided. So, higher powers of 2 cannot divides.

So, all the other factors of 2 will collect themselves and go and divide a plus 1, similarly if we have the other case that 4 divides a minus 1 then 2 power e minus 1 will have to divide a minus 1 and a plus 1 in this case is congruent to 2 mod 4. So, this is what we have obtained that if a is a solution to x square congruent to 1 mod 2 power e, then a plus minus 1 has to be divisible by 2 power e minus 1.

(Refer Slide Time: 24:32)



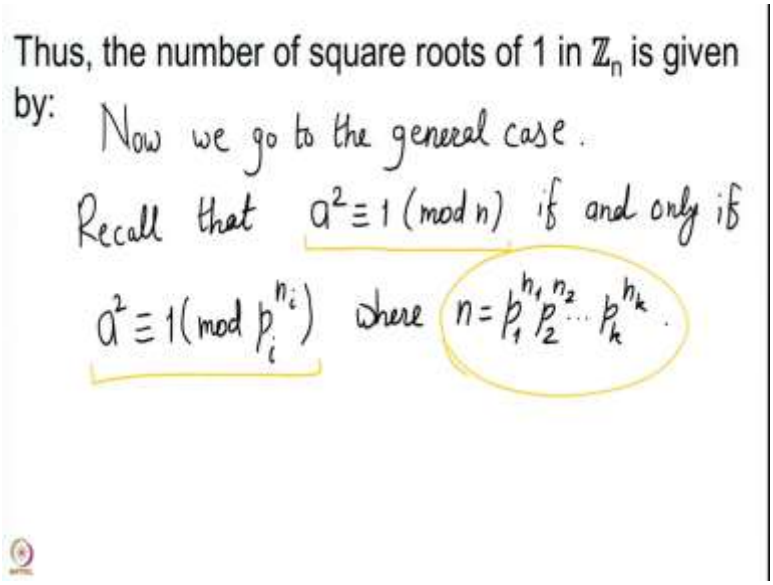
So, thus a in the natural numbers is a solution to x square congruent to 1 mod 2 power e and remember we are in this case, then a is congruent to 1 modulo 2 power e minus 1, or a is congruent to minus 1 modulo 2 power e minus 1. So, when we look at the whole set of numbers where we begin this is 0, which we ignore then we have 1, then 2 and so on, this is where we have 2 power e and somewhere exactly in the middle we have 2 power e minus 1.

So, the first case tells us that a has to be congruent to 1 mod 2 power e minus 1. So, that can be this number 2 power e minus 1 plus 1, or it can be this number, a equal to 1 both are 1 modulo 2 power e minus 1. The second case which says that a is minus 1 modulo 2 power e minus 1 will

tell you that it can either be 2 power whole e minus 1 or this quantity which is 2 power e minus 1, minus 1. These are the only 4 solutions in the case when the power of 2 is more than 4.

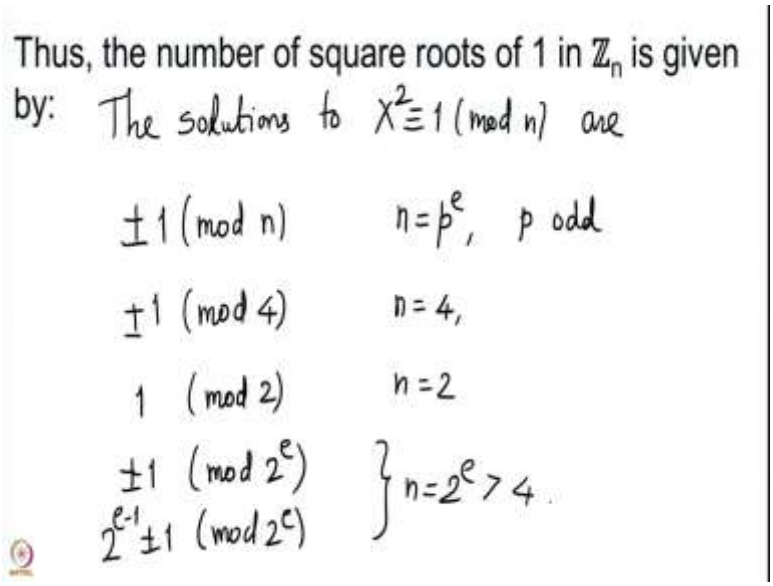
So, we have now obtained all solution, we have solved all the cases when n is a prime power, when p is odd, there are only two solutions, when n is a power of 2 but equal to 2 itself, then there is only one solution, if n is 4 then there are two solutions and when n is a power of 2 but strictly bigger than 4 then we see that there are 4 solutions. Now, we want to go back to our general situation and compute the number of solutions to x square congruent to 1 modulo n.

(Refer Slide Time: 27:06)



So, that is the case that we want to now do. So, now we go to the general case, so recall that a square is congruent to 1 mod n, if and only if a square is congruent to 1 mod pi power ni where we have this prime factorization. So, we start with this prime factorization to begin with to rephrase the statement we would begin with this, then we have that a square congruent to 1 mode n holds if and only if a square congruent to 1 mod pi power ni holds.

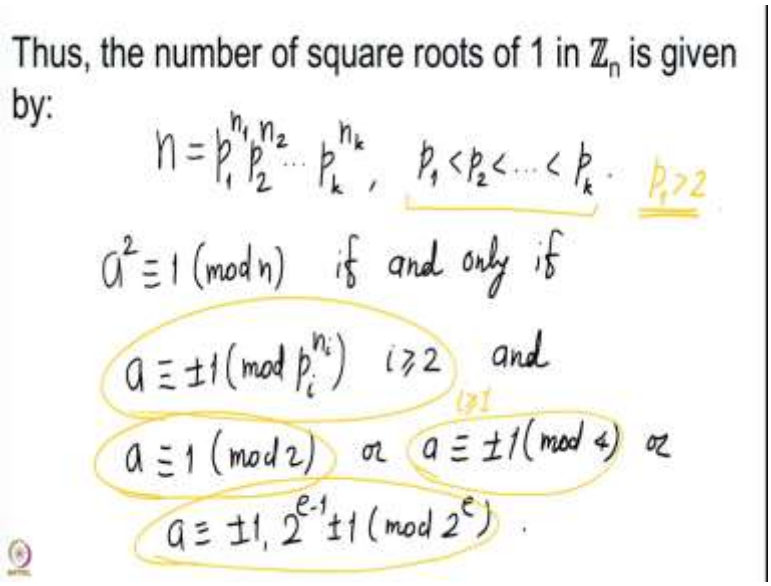
(Refer Slide Time: 28:22)



Now, the condition that a square is congruent to 1 mod pi power ni can be written in terms of linear congruencies, this is because we have solved the cases a square congruent to 1 mod pi power ni. So, these cases let me just summarized them in the next slide for you in the following way.

So, these solutions to x square congruent to 1 mod n are plus or minus 1 mod n, when you have n to be p power e, and p is odd, another case is when you have just 1 or minus 1 modulo 4 ofcourse you have n equal to 4, modulo 2 you have only one solution. And in the final case when you are looking at 2 power e, then we have these 4 solutions. So, we will take our n write its prime power factorization also put the pi in the increasing order. So, p 1 less than p 2 less than dot, dot, dot.

(Refer Slide Time: 30:18)



Then we will look at so this is what we do n equal to p 1 power n 1, p 2 power n 2 up to pk power nk and we write it in this way. Then we know that for obtaining the square. So, a square congruent to 1 mod n if and only if a equal to plus or minus 1 mod pi power ni for i bigger than or equal to 2 and then there are these bunch of solutions.

So, a equal to 1 mod 2, or a equal to plus or 1 mod 4, or a congruent to plus minus 1, 2 power e minus 1 plus minus 1 mod 2 power e, these are the only possibilities. So, we will combine these in all the cases, suppose that there is no prime equal to 2 in the factorization. Then we have only this case and in fact then you will have i equal to 1 and ahead.

So, we are going to get two possibilities for each prime, when we write them all together you have 2 power k possibilities, you have 2 power k linear congruence's, there are going to be simultaneous systems of linear congruence's, which are given by plus or minus 1 modulo each pi power ni. And there are unique solutions modulo the product of these module i which is n. And so you are going to get exactly 2 power k solution.

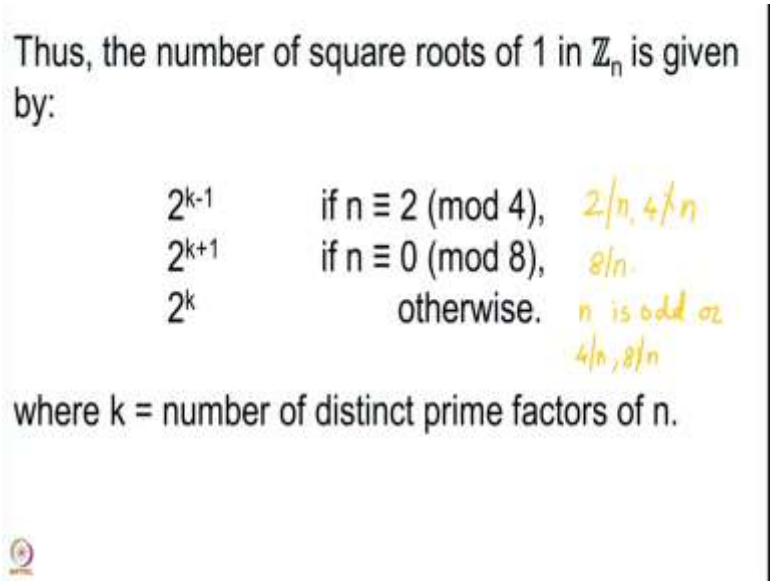
So, there are exactly 2 power k solutions, when 2 does not divide your number, when 2 to divides your number there are two possibilities, 2 divides but 4 does not divide, 4 divides but 8 does not divide and 8 divides it. So, depending on these three cases we have three possibilities

once again when 2 divides but 4 does not divide, then we will be in this case 2 divides but 4 does not divides.

So, we are in this case and in this case there are no there is a single equation. So, you have k primes dividing n the 2 onwards p2 up to pk, these are the k minus1 primes, they give you 2 power k minus 1 systems of solve simultaneous linear congruences and for 2 there is no condition except that a be congruent to 1 mod 2. So, there is only 1 congruence given here for 2 and then there are varying congruencies for pi power ni whenever pi are odd.

So, you get exactly 2 power k minus 1 solutions, when you are looking at 4 divides but 8 does not divide, then you have again 2 power k solutions, because this behaves like the power of odd primes. And when you have 8 divides, then you actually have 4 congruence. So, you are equations have now 2 possibilities modulo odd primes, but 4 possibilities modulo 2 power. So, you have 2 power k plus 1 solutions.

(Refer Slide Time: 34:23)



So, when we write it in the summary, we have that whenever 2 divides 8, 4 does not divide that is the case number 1 and we see that in this case 2 divides n and 4 does not divide n, in this case we have exactly 2 power k minus 1 solutions, here either n is odd or 4 divides n and 8 does not divide n, in this case we have exactly 2 power k solutions and this is the case where 8 divides n.

So, this has been a somewhat intricate analysis of computing the square roots of 1 in Z power n z. We will be looking at some simpler things now once you we begin our next lecture. So, think about this, this is not very difficult it is only slightly intricate. But if you read it carefully if you solve all the things carefully I am sure you will get it. I hope to see you in the next lecture thank you.