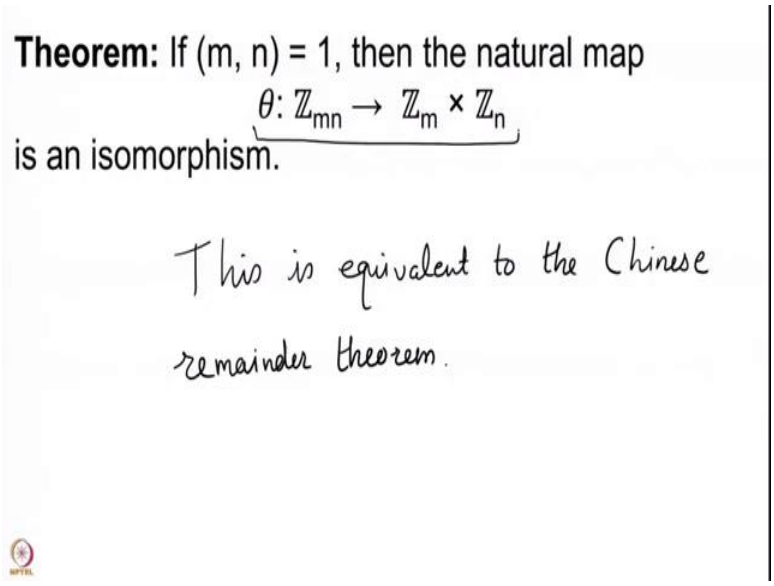
A Basic Course in number Theory
Professor Shripad Garge
Indian Institute of Technology, Bombay
Department of mathematics
Lecture-30
Structure of Un - II

Welcome back, we are looking at the structure of Un in general, the group of units modulo any given natural number n. And we saw that we can use the Chinese Remainder Theorem to understand it.

(Refer Slide Time: 0:36)



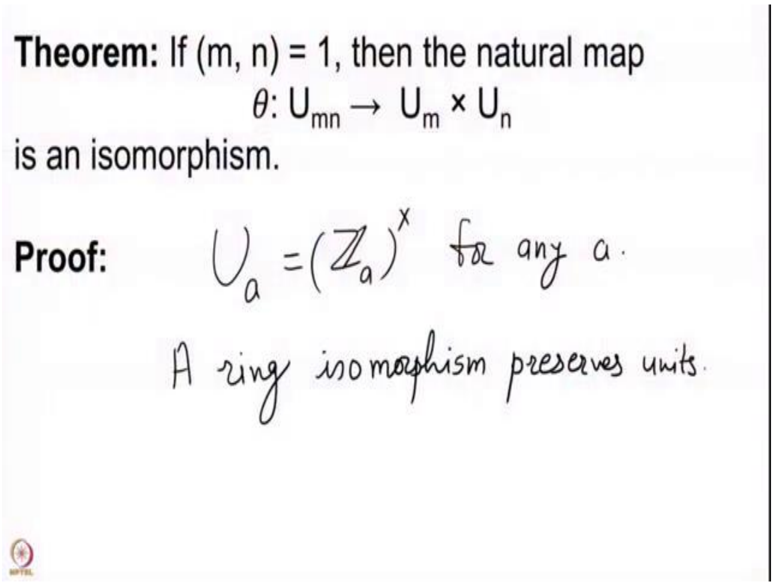
So, let us recall quickly we have here the slide which writes a statement that we have. And we observed in the last lecture that this is equivalent to the Chinese Remainder Theorem. So, the statements says that whenever you have m and n to be a pair of natural numbers which are co prime to each other, then there is an isomorphism, actually a ring isomorphism from the residue classes modulo mn to the products of the residue classes modulo m with the residue classes modulo n.

And this ring isomorphism is the natural map that we can think about, which is that you start with a residue class of some natural number a modulo mn and we send it to the residue plus modulo m residue class modulo n of the same A. This is the map which gives you an isomorphism. Now, this is a ring isomorphism, so as we have observed it will take sums to sums and products to products. So, there is 1 more thing about the isomorphisms which is that it will take the identity element to the identity element.

Note that in the ring homomorphism identity, the multiplicative identity need not always go to the multiplicative identity. But let us not worry about that right now. Here this is an isomorphism and so, it should take the multiplicative identity 1 to the multiplicative identity to the product of those 2 rings, which will then have to be 1 comma 1. Whenever you have 2 rings r 1 and r 2, then in the product r1 cross r 2 the 1 of r1 cross 1 of r 2, that or 1 comma 1 of r1 comma 1 of r 2 that element is the multiplicative identity for r1 cross r2.

So, the element 1 should go to 1 comma 1 and that is also true 4 as the, by the way, we have defined our map, we will take the element 1 in Z mn, which is the resolution of 1 and that goes to the residue class of 1 modulo m comma residue class of 1 modulo n. So, identity goes to identity and then 1 can prove that if something is invertible, its image is also invertible. Because if I have an element U here, it will say go to U 1 comma U 2 and U has inverse V, which goes to v 1 comma v 2, then because U v is 1, it will tell you that U 1 v 1 is 1 and U 2 v 2 is 1. So, the ring isomorphism has this nice property that it will take the units which are the invertible elements, modulo in with respect to the multiplication to the units. And we just observe this to get our next result.

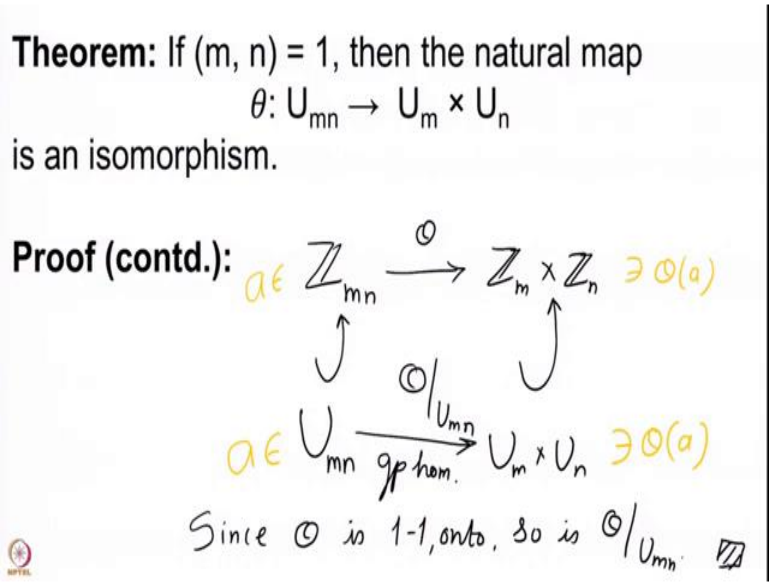
(Refer Slide Time: 3:54)



So, what we have is that, Ua is basically the group of units in Z a, for any natural number a and a ring isomorphism preserves units. So, this very simple fact, that a unit has to go to units under a ring isomorphism, we get that when you restrict the map theta to the group of units, you get a group isomorphism. Of course, now, the group of units is not preserved under the addition, we know that 1 is always a unit, minus 1 is always a unit and if you take the sum of these two, you get 0 and 0 is never a unit.

So, this is not preserved under addition, but there is the multiplication structure defined on U and the set U m is actually a group with respect to this multiplication coming from the finite ring Zn. And when we have that theta from Zmn to Zm cross Zn is a ring isomorphism we simply restrict it, so the to give you a flavor of some advanced mathematics.

(Refer Slide Time: 5:24)

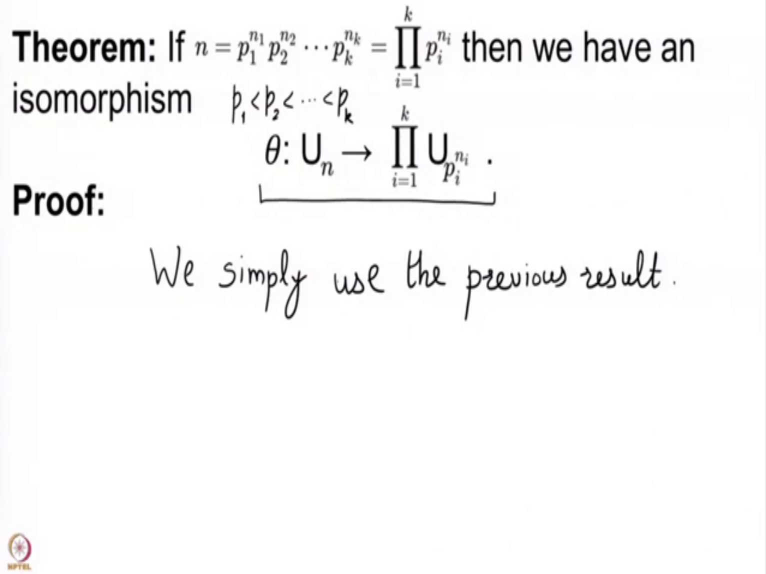


Or the way this advanced mathematics is done is done by looking at these commutative diagrams. So, we have, this is the map theta, we have U mn sitting here, we have U m cross U n sitting here, we observe that if you take an element a in U mn, then you will look at a in Z mn. So, theta a is an element in the right hand side Z m cross Z n, but since a is invertible theta a is also invertible. So, it is in the product of the invertible elements in the corresponding rings.

And therefore, we have defined the map theta having restricted the theta to Umn. So, we have a map, a group homomorphism, so this is a group hom and we need to just observe now that it is a 1 to 1 onto map, but that is clear because the original theta is 1 to 1, onto. So, since theta is 1 to 1, onto, so is theta restricted to Umn. So, whenever I have any n, any natural number n, the U n can be understood if you can decompose n as product of elements which are co prime to each other, pairwise co prime to each other.

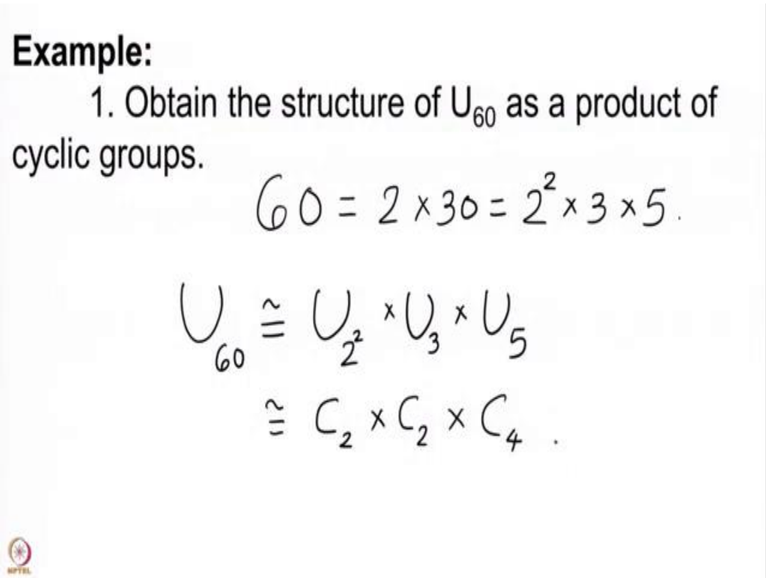
But we know no better such factorization than the prime factorization. So, what we do is that we decompose n as product of primes, collect all the same primes together, so we get one very nice decomposition for n.

(Refer Slide Time: 7:29)



Here we have this decomposition for n where the primes are of course arranged in the increasing order. So, we have p 1 less than p 2 less than dot dot dot pk. So, they are not just that they are distinct but they are put in some nice order, then the map theta actually is an isomorphism of groups. And this is a corollary, we simply use the previous result. So, once we have understood U pi power ni, 4all primes pi, then we have understood using this result the structure of all Un. It is a good thing to have done it as a result, but we should also do the examples with respect to this. So, let us see some examples.

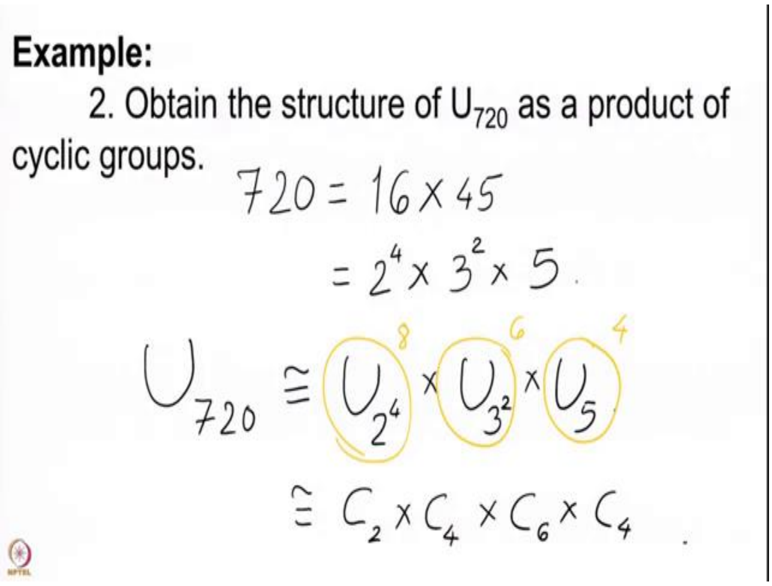
(Refer Slide Time: 8:42)



Let us try to compute the structure of U60 as a product top cyclic groups, this is something more than writing U60 as product of Upi power ni, because we need to also identify when each of those pi power ni are cyclic, or whether they are themselves further product of cyclic groups, that is something that we have to observe. So, we write 60 in terms of its prime factorization, we will have 2 into 30. You can take one more 2 from 30 to write it as 2 square into 15 and 15 is 3 into 5. So, we have that U60 is isomorphic to U 2 square into U 3 into U 5.

We observed already that U4 is a cyclic group of order 2, so this is C 2. U 3 is already cyclic, its order is 5 3, which is 2. And U 5 is also cyclic, its order being 5 5, which is 4. So, we have a complete description of U60 as product of cyclic groups. One will have to be careful when the power of 2 dividing the number n is more than 4. So, let us do one more example.

(Refer Slide Time: 10:16)



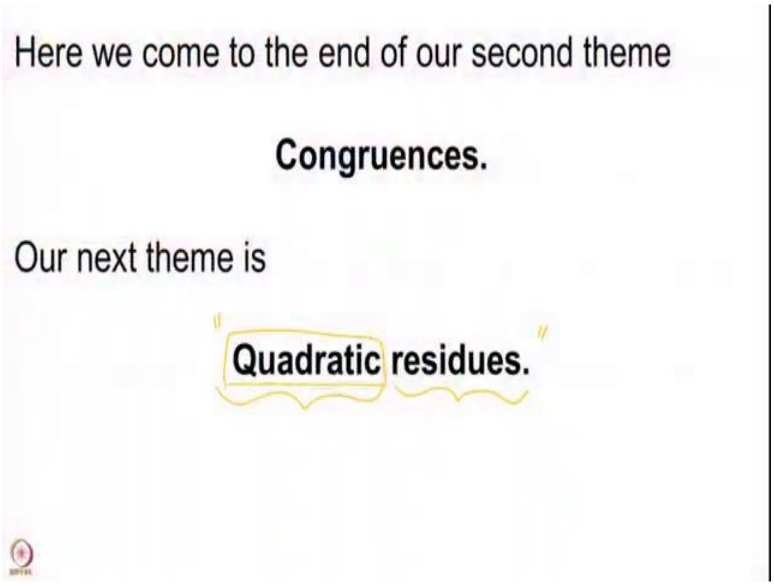
Here we want to understand the structure of U720 as a product of cyclic groups. So, we will need to write 720 as Prime powers product of prime powers. So, clearly 720 is 72 into 10 and 72 is 8 into 9. So, 8 is the highest power of 2 which divides 72 and therefore, 16 is the highest power of 2 which divides 720. So, remember we had got 10 as 2 into 5 and then we had 9 here, so this is 16 into 45, which gives us 2 power 4 into, now 45 has 9 dividing it so we have 3 square, and then we have 5.

This is the prime factorization of 720. And therefore, U720 is isomorphic to U 2 power 4, cross U 3 square cross U 5, but U2 powers 4 the U 16, remember, this is a product of two cyclic groups, one of them being c 2, and then the other is of order 4. Because the cardinality of this group the cardinality here is 8, the cardinality here is 6 and the cardinality here is 4.

So, for 8, once we know that it has to be a product of C2 with some another cyclic group, we know that it has to be C2 cross C4.

This is a prime power where p is odd, so this is already cyclic and this is also cyclic. So, this is the complete description of U 720. And what we have done so, far is that we have understood all U n modulo some basic results in group theory. And this is how we come to the end of our second theme.

(Refer Slide Time: 12:43)

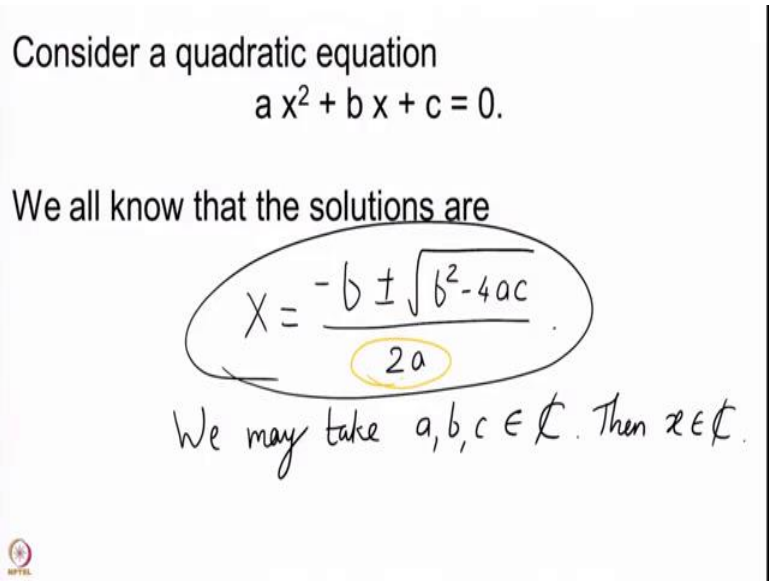


Remember, we are looking at some special themes in this basic course on number theory. Our very first theme was on primes where we understood how primes were defined, how we could get a unique factorization of any natural number in terms of primes, and we looked at some very basic properties of primes. Second theme is this theme on congruences, where we looked at, we defined what we mean by congruence. And so, we looked at the ring Z n, Z modulo n Z.

And we have tried to understand this ring as much as possible, the structure of this ring, not just by understanding the addition, but also the product and we have just now completed the understanding of all units in these rings. So, this completes our study of congresses, although we are going to study congruences further. You will often see that the themes that we have studied earlier will continue to be useful in higher themes. So, the thing that we have done earlier is not going to be forgotten.

We are going to use lots of things about congruences and some may even argue that you are going to do congruences for what you are going to do later. But it is going to be with some special focus on quadratic equations. And therefore, this is the theme which we call quadratic residues. This is the next theme that we are going to now do. So, quadratic residues, comes with quadratic. Residues say that this has to be something to do with congruences because we are looking at residue classes and so on, so that will tell you that residues have something to do with congruences. But let us study the notion quadratic first.

(Refer Slide Time: 14:43)

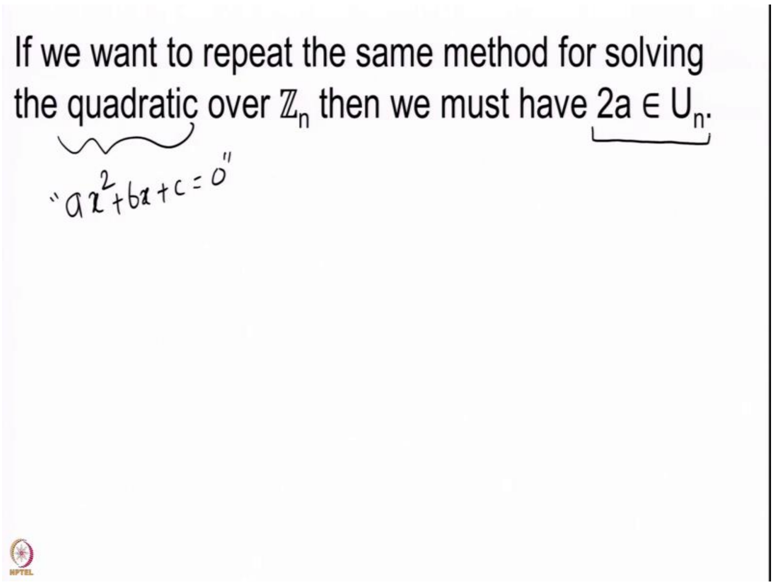


Whenever you hear the word quadratic, the thing that comes to your mind first is the quadratic equation, which is a x square plus b x plus c equal to 0. This is the equation that we all think about, we also know how to solve this equation. Let me just quickly recall the solution of this. This is the formula that we have all been studying since school. So, this is given by minus b plus or minus under root b square minus 4 ac up on 2a. This equation I have not told you where a, b, c come from, so we may take the coefficients a, b, c to come from complex numbers for instance.

And then we know that our solutions will also belong to complex numbers, then the solutions x given by the above formula are also complex numbers. You may take a, b, c coming from integers, rationales or even reals. But that does not guarantee that the solutions will always be in those particular sets. However, we know that whenever a, b, c are taken from complex numbers, then the solutions can always be found in complex numbers.

If you wanted to do this for the sets Z n, then what should we do? First of all, we note that this formula is a somewhat symbolic formula. You know, we do not really use where a, b, c come from, as long as you have a product for the a, b, c and x defined, putting this value back here, you will get a solution. But when you are applying this for some particular sets, then you have to be careful because if you are dividing by 2 a, then you should say that my 2 a is an invertible element, this is something that we will have to begin with.

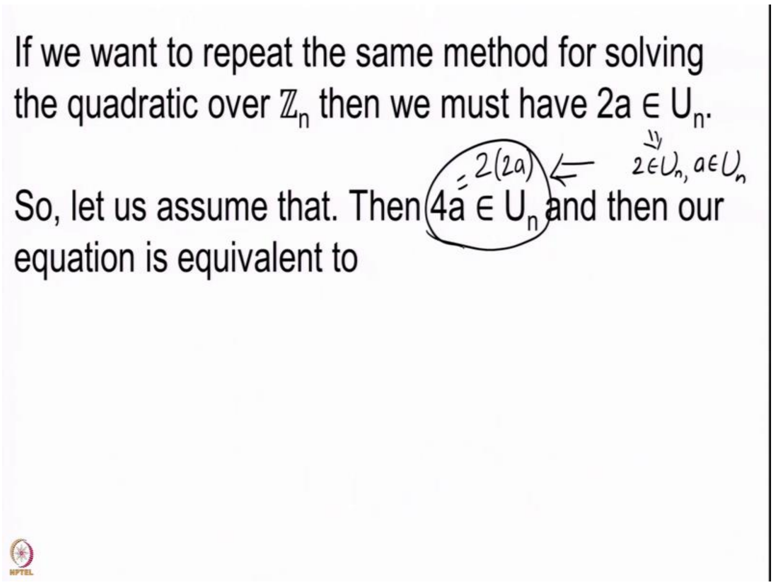
(Refer Slide Time: 17:02)

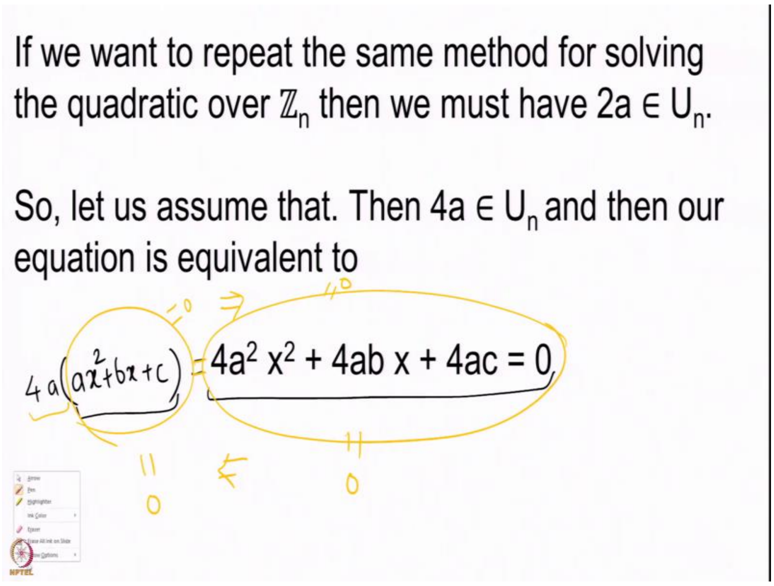


So, if we want to repeat this same method for solving the given quadratic, remember the quadratic that was given to us, the quadratic is a x square plus b x plus c equal to 0, this is the quadratic equation that we want to solve over Z n, then we must have that 2 a is an invertible element. If you want to use the same method, the same formula, then we should first of all have that 2a is invertible in modulo n. Which means in the language of the GCDs, which is something we have developed in our very first theme, that the GCD of 2 a comma n has to be 1.

Then n cannot be even and will have to be an odd element and further the element a has to be co prime with n. So, these are the standing assumptions that we have. So, let us assume this, what we are assuming is that 2 a is an invertible element modulo n. If 2 a is invertible, we have just now seen that 2 has to be invertible and a has to be invertible.

(Refer Slide Time: 18:41)

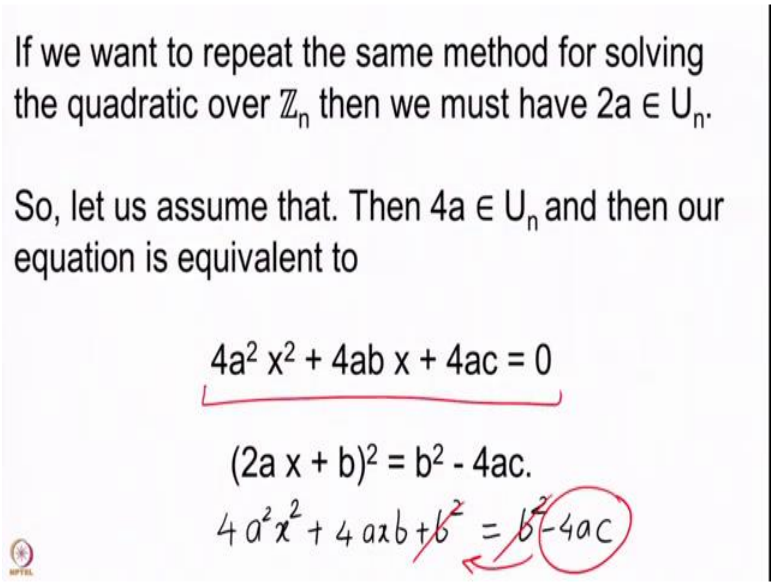




So, what we then get is that 4 a is also invertible, because 4 a can be written as this is 2 into 2 a and this already implies that 2 belongs to Un a belongs to Un. If 2 is there in Un, then we get that 4a belongs to U n and then our equation is equivalent to the following equation, 4 a square x square plus 4 a b x plus 4 ac equal to 0. This is because this is simply 4a into the equation that we started with. Whenever you have a solution to this equation, you have a solution to this equation whenever this is 0. Whenever this is 0, this has to be 0 because these two are identified by multiplying by an inverse, by an invertible element.

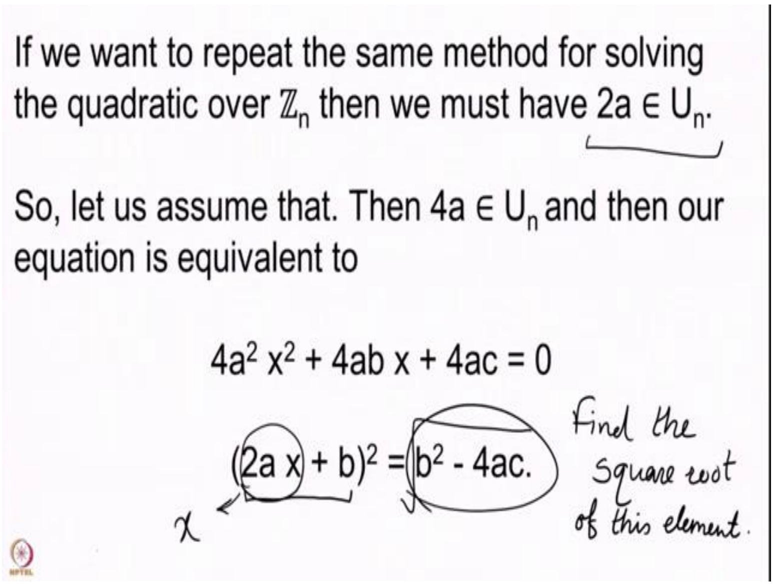
So, this is 0 implies that this is 0. On the other hand, if this is 0, you will simply multiply by 4a to get that this is 0. So, our equation is indeed equivalent to the equation that we have written down and now we know how to deal with these things. If you remember the proof of your quadratic formula, then you know that you have to separate the squares. So the squares need to be separated.

(Refer Slide Time: 20:18)



And once you separate the squares, we get our formula. Let us just check that the squares on this side are 4a square x square plus 4 a x b plus b square and on this side you have 4 b square minus 4 ac. We will cancel the b square on both sides and bring this minus 4 ac to this side to get the equation that we have.

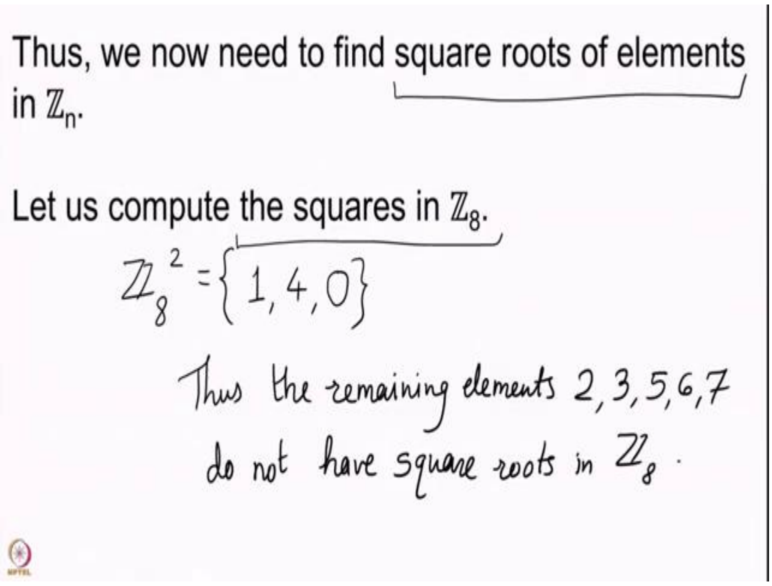
(Refer Slide Time: 21:23)



So, the equation 4a square x square plus 4 ab x plus 4 ac equal to 0 is equivalent to the equation that we have found here. And therefore, what we then have to do is to find the square root of this element. Because once you find the square root, you would have found values for this, you can subtract b to get the value for 2 a x, but 2a is invertible, that is something that we have already assumed. So, once you have the value for 2a x, you can compute the value of x. This is precisely what we have done in the quadratic formula.

We would compute the square root of this number, b square minus 4 ac, subtract b, of course, the square root comes with 2 signs, because there is no unique square root, there can be a plus minus, and then you divide by 2 A. This is the same method that we are going to apply. But this whole method hinges on the possibility of finding square roots of given elements in Z n.

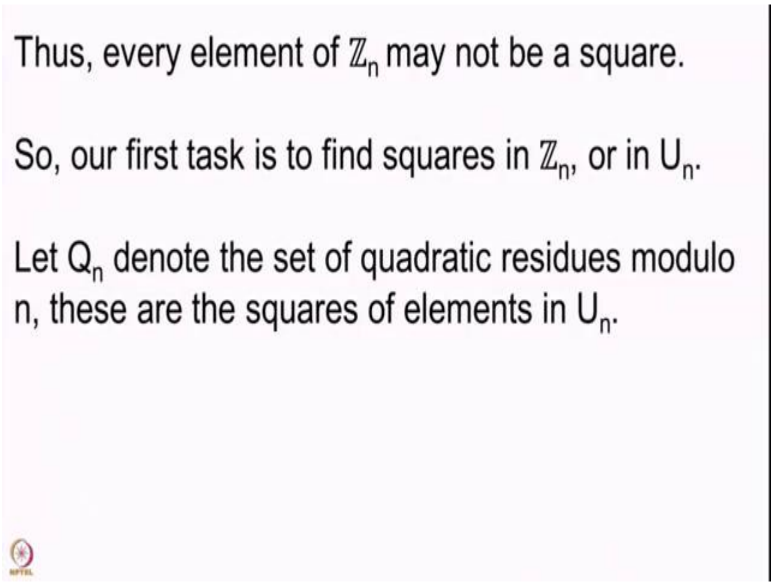
(Refer Slide Time: 22:40)



So, what we need to do is to find square roots of elements in Z n. Is it so easy to find the square roots of elements, are all elements there which have square roots, or do we have to make some cases about them? So, let us do one Example. Let us compute squares in Z 8. So, to find square roots of elements, we need to find what elements have square roots. And this can be done by simply computing the squares. So, if you write the elements of Z 8 and then we compute the squares, 1 square is 1, 2 square is 4, 3 square is also 1, because 3 square is 9, modulo 8 it is 1, 4 square is 16, which is 0, 5 Square is 1, 25 is 1, 6 square is 36, but modulo 8 it is again 4, 7 square is 1 and 8 square is 0.

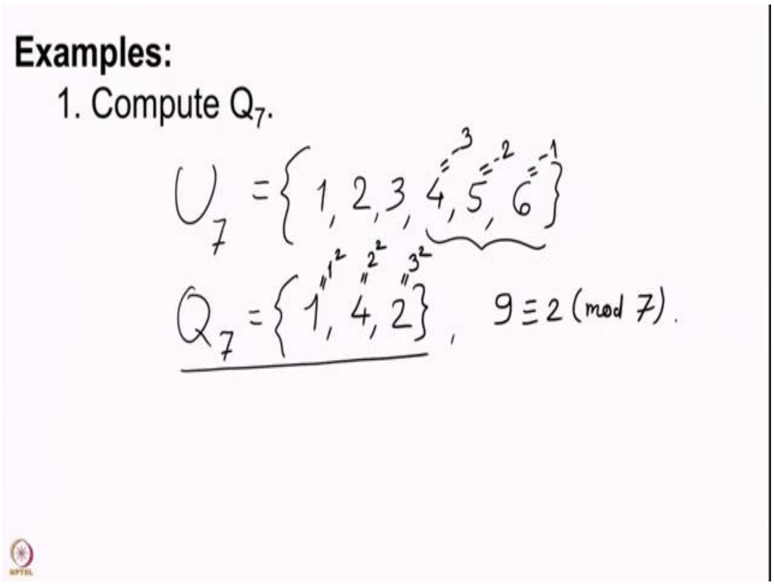
So, these are the only squares in Z8. Thus, the remaining elements 2, 3, 5, 6, 7 do not have square roots in Z 8. So actually, our elements 3, 5 and 7, these are units. Even for units we do not have square roots. The elements which are non units 2 and 6, we can understand them not having square roots in some way. But we would try to at, we would like to at least understand which of the units have square roots. So, this is something that we would now like to do.

(Refer Slide Time: 25:10)



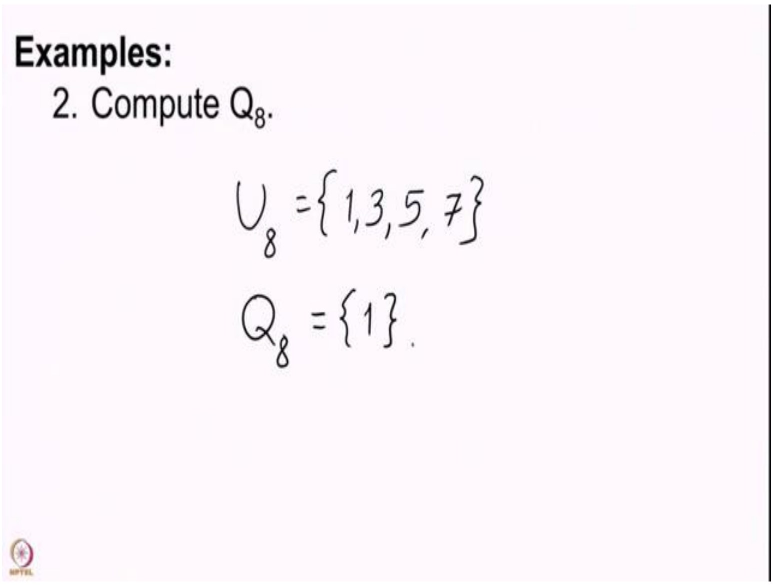
We would like to find elements which have square roots in Un and our task is to find square in Z n or squares in U n. So, we call that set to be Qn. So, Q n denotes our set of quadratic residues modulo n. These are the squares of elements in U n, we would like to compute these Q n, see whether there are methods for computing the elements which are squares in Un. Of course, our experience tells us that you should look at Up's first or Up power e first, perhaps deal with the case U2 power e separately and then you try to get the hang of the set Q and in general. But let us see whether we can do some simple calculations and try to find the squares in Q 7.

(Refer Slide Time: 26:04)



So, what are the squares in Q 7? We need to find U 7 first. U 7 is simply all elements which are co prime to 7. So, these are the 3 elements and then Q 7 is going to be the product of these elements. So, 1 square is 1, 2 square is 4 and 3 square is 9, which is 2 modulo 7. So, thus we have that these are the only squares. This is square of 1, this is square of 2, this is square of 3, all the 3 other remaining elements are negative of these three. So, 4 for instance is minus 3, 5 is minus 2, and 6 is minus 1. So, the squares of these 3 elements will coincide with the squares that we have. This is the complete answer for Q 7.

(Refer Slide Time: 27:07)



We have already computed Q 8. And let me just tell you that when you were looking at U 8, we had all odd elements here, but Q8 only one element. So, indeed, the case for n equal to 2 power e needs to be done with separately, dealt with separately and the remaining cases can perhaps be dealt separately, hopefully and in a simpler way. We will look more for this formally and these competitions in the coming lectures. So, see you in those lectures. Thank you.