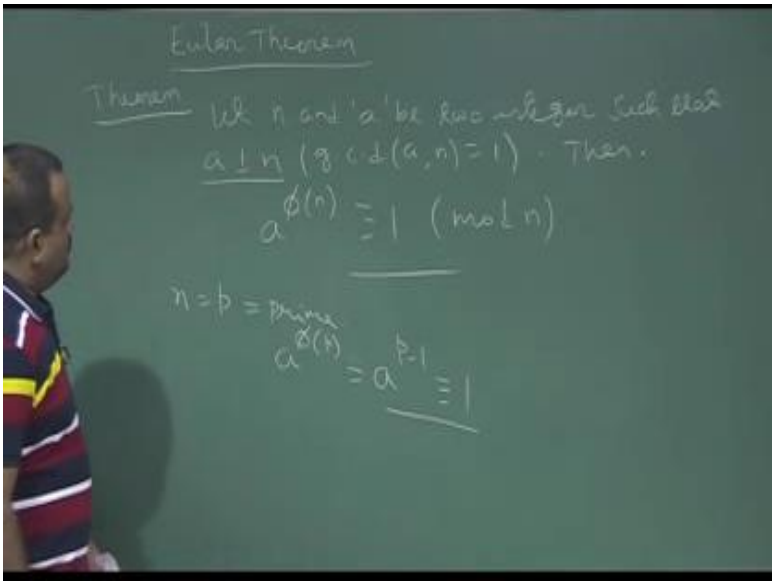
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 19
Euler's Theorem, Quadratic Residue

We talk about Euler's theorem here.

(Refer Slide Time: 00:27)

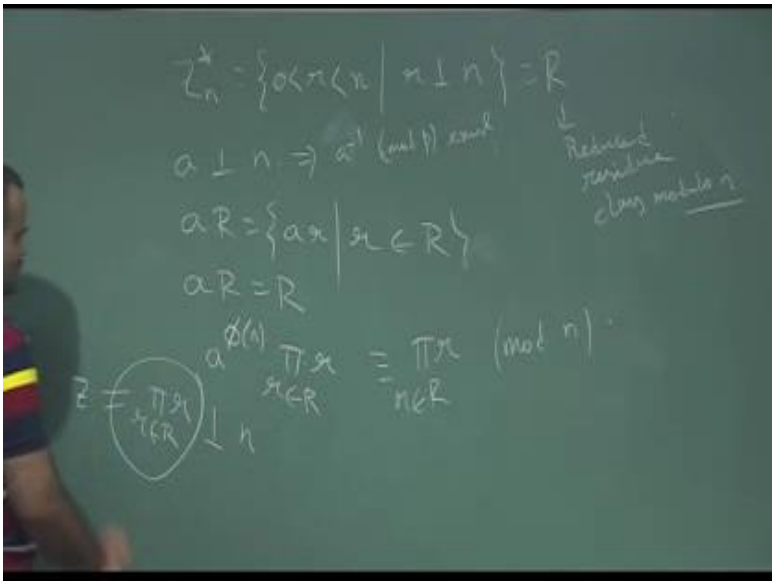


So, let us just write the statement of the Euler's theorem. Euler's theorem is telling let n and a be two integer such that; that means, gcd of n is 1, then a to the power phi n is basically congruent to 1 mod n. So, this is the statement of Euler's theorem.

So, we take a integer n and we take a integer a such that they are relatively prime then gcd of this is 1. So, if you take n to be prime if n is p which is prime set then phi to the power p which is basically what this we know phi p phi p is p minus 1 phi functional then this is basically 1 this is coming from Fermat's little theorem. But this is a particular Fermat's little theorem is a particular case of Euler's theorem, but a Fermat's little theorem was invented before this Euler's result came into the literature. So, we are going to prove it in general way that this phi of this is basically phi of n is congruent to 1 mod n.

So, how to prove this? To prove this we need to take help of what is called reduce residue class, the r.

(Refer Slide Time: 02:38)



So we have n; n is the number integer, so we defined we know this Z n star this is basically set of all integer which are h nonzero; non zero positive integer which are less than n such that they are co prime to n this set. And this cardinality of this set is basically phi of n. And this set is also denoted by r, this is called reduce residue class modulo n.

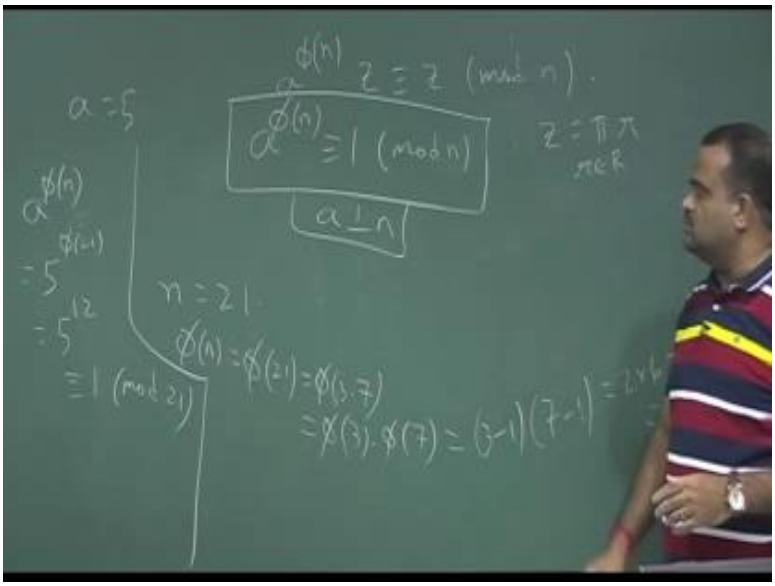
So now if a is independent with n, independent means co prime to n; if a is co prime to n then if we define this a r; a r is basically a into r and r is coming from this set now we have seen this a R is basically R. Since a is co prime with n, because if you take any two. So, this set is basically what? This set is basically if you take any two element from this set say n a and which is sorry; n a which is congruent to say m a mod n sorry n is there. So, we cannot use n, so x y you can use. Suppose we take any two element f here say x y. So, x a is congruent to y a mod n.

Now, since this is independent these imply a inverse exists mod n and we can find this inverse by extended Euclidean algorithm. So, we can multiply a inverse both sides. So, this will give us x is congruent to y mod n. So, any two elements here are, so these elements here are basically congruence of the elements over here in some order. So, basically a R is equal to R. So, what we do? We multiply all the elements of a R. So, we multiply all the elements of a R, so this is basically we denote by R star sorry.

So, a R is basically R and the number of element over here is we know this is the phi n, so if we multiply all the elements from this a R, so this will be of the form a to the power phi n into r, r is coming from this R. And this must be congruent to; since this is the all the element we are multiplying from this set and this must be equal to pi of r, because these two set are same may not be in the exacts the order we are having. So, maybe in the different order they are under congruence operation. So, this is the result under mod n.

So, now, here in this all the elements over here in r are basically co prime with n. That means, all the product is also basically co prime with n, so that mans this inverse exists under mod n. So, we can multiply this by this inverse of this so this we denote by say Z.

(Refer Slide Time: 07:09)



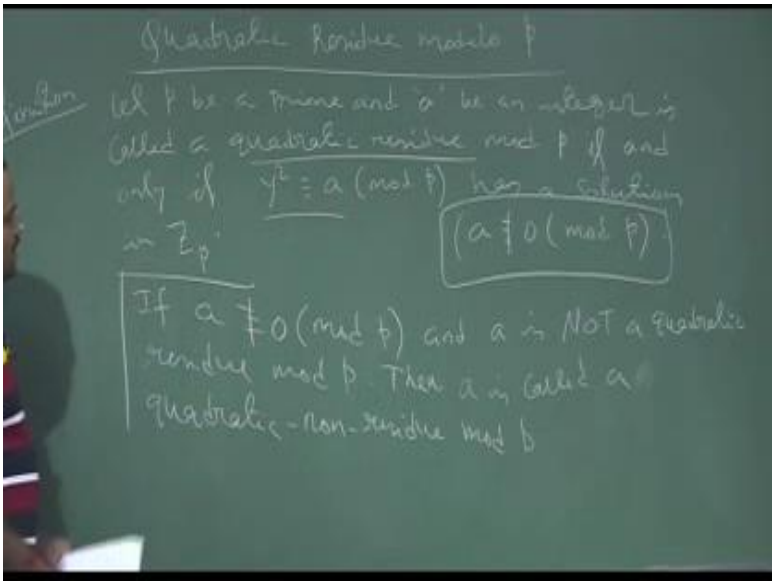
So, this is basically we have a to the power phi n into Z is congruent to Z mod n, our Z is basically r. Now all the elements over here is; if r belongs to capital R then r is independent with n so; that means, all the elements are independent with n; so that means Z is this independent, independent means relatively prime. The symbols we use for relatively prime or co prime that means Z inverse exists mod n exist. So, we multiply Z inverse on both side we will be getting r n is congruent to 1 mod n. So, this is the Euler's theorem, we prove the Euler's theorem. So, this is true for any integer n and integer a such that a is relatively prime with n. So, this condition must be there for this result could be hold.

So, let us take an example. So, these examples say we would again is equal to say 21. So, then what is phi n? Phi n is basically; so 21 can be written as phi of, sorry this is phi 3 phi 7 phi 3; 3 on 7 so this is these are in relatively prime so we can use that. Now this two are prime numbers, so for prime number we know this result so this is basically. So, this is basically 3 minus 1 into 7 minus 1. So, this is 2 into 6 into 12.

Now, we take a, a which is basically relatively prime with 21. So, if you take a is equal to 5. Then a to the power phi n is basically 5 to the power phi of 21 this is 12 basically this is basically phi of 21 is 12. So, phi of 21 which is basically 12 and we can easily verify that this is congruent to 1 mod n. So, this is an example of Euler's theorem. And we have seen the Fermat's little theorem is a particular case of Euler's theorem.

So, these will use in many cryptographic protocols like RSA many many cryptographic algorithms RSA. So, to prove correctness of RSA we need to have this theorem in our hand. So now, we will define what is called quadratic residue modulo some prime p.

(Refer Slide Time: 11:08)

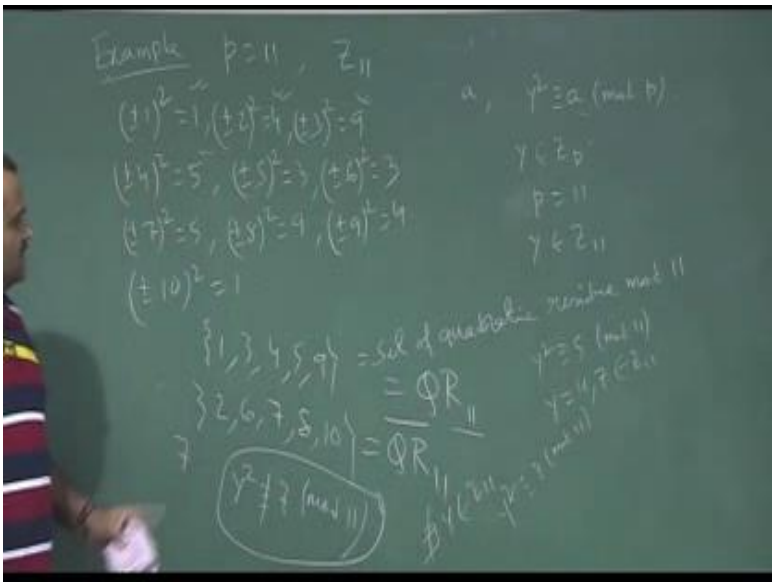


So, we define the term quadratic residue modulo p, where p is a prime. So, how to define this definition? Definition of the quadratic residue, so let p be a prime number and a be an integer. Now we define a is called integer, is called a quadratic residue mod p if and only if the congruence equation y square equal to a mod p has a solution in Z p.

And here a must be a is not congruent to 0 mod p so that means a is not a multiple of p; a is congruent to zero mod p means a is either p 2, p 3, p like this so we are not allowing this. So, a is not a multiple of p. That means, a has a square root. So, that square root is basically y. So, a has a square root and that is basically y, then if this equation is has a solution then we call this as a square quadratic residue mod p. Now when we say it is a quadratic non residue? If this equation has no solution, if n is not a multiple of p and a is not a quadratic residue mod p then a called a quadratic non residue mod p. This is we say is not a quadratic residue then we called there is a quadratic non residue.

We will take some example. Suppose we take a prime number p say p is equal to 11. So, so there are many cryptographic algorithms which are based on this quadratic residue. So, this has good importance in cryptographic protocol.

(Refer Slide Time: 15:28)



So, let us take p to be example. So, let us take p to be 11, so we are in Z 11. So, we are talking about quadratic residue under mod 11, so we are in Z 11. So now, if we take the possible y's. So, basically a a we are looking for a quadratic residue in Z 11. So, we are looking for a such that y square equal to congruent to mod p. So, then a a is a quadratic residue and this y is sort of square root of a kind of as if we are squaring a, we are finding the square root of a. So, that means, we are looking for possible y's so that if y exists such a y exist in Z p then we called a is a quadratic residue; that means, a can be square root I mean a a has a square root. So, a is called quadratic residue.

So, if we try for all possible y's kind of things, so this is basically 1, so these are all under mod 11 operations. So, plus minus 2 square this is basically 4, plus minus 3 square this is 9, plus minus 4 square this is 16 then 16 mod 11 is basically 5, plus minus 5 square this is basically 25; so 25 mod 11 is basically 3, plus minus 6 square. So, these are the possible y's this plus minus 5 plus minus 6 are basically 36 mod 11 is 3. Plus minus 7 square is basically 5. These are all under mod 11 plus minus 8 squares. This is basically 9 plus minus 9 square, it is basically 4. Plus minus 10 square it is basically 1.

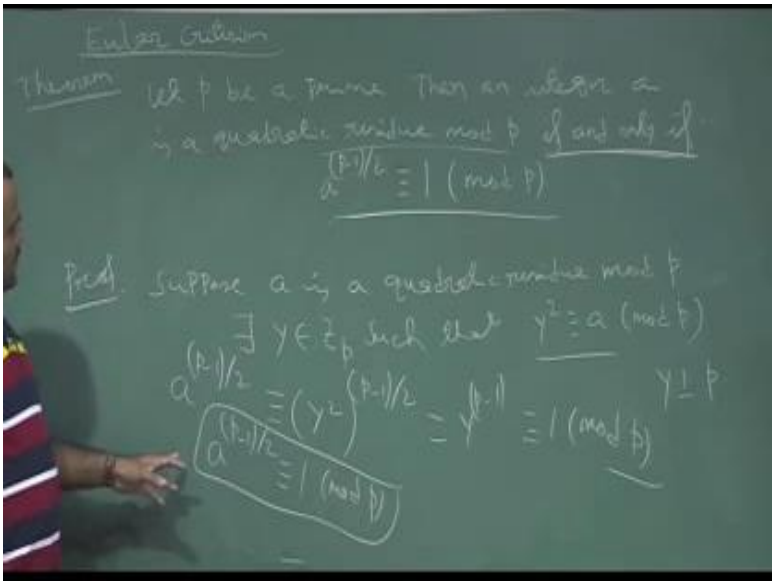
So, these are possible y's basically. So, y must so p is 11. So, y must come from this side basically Z 11. So, these are possible y's, so that means these are the quadratic residue. So basically, this set 1 2 is not 3, 4, 5, 9. So, this set these are all the elements over here are set of all quadratic residue mod 11. So, these are all quadratic residue under mod 11. So, this is denoted by basically you can denote by QR 11; quadratic residue mod 11. That means remaining are the quadratic non residue mod 11. So, any element because 4 is a quadratic for a a is equal to 4, 4 is a quantity residue mod 11 because for 4 we have a y. So, if you take y square is congruent to 4 mod 11; that means y is basically plus minus 2, plus minus 2 is basically 9. So, the y is basically 2 and 9 that means 4 has square root. So, these are the possible values of y.

So, for this y if you squared it then take the mod 11 it will give us 4. So, any element over here has a square root. So this is the 4, if you taking a 5 also; for 5 if you want to find out y square is congruent to 5 mod 11 then. So, what is y? Y is either; so 5 is giving us 5 4 and minus 4 7 and minus 7. So, minus 7 is 4 basically under mod 11 and minus 4 is equal to 7. So, this is basically 4 and 7 which are coming from Z 11. So, these are all quadratic residue mod 11.

Now, who are the quadratic non residues? So, the remaining set like 2, 4, 5 is there 6, 7, 8, 10. So, these are all quadratic non residue mod 11, because if you take any you say for example; if a is equal to 7 then they are does not exist a y such that y square is congruent to 7 mod 11. So, this system has no solutions because there is no such y, there does not exist y in Z 11 such that y square will give us 7 mod 11. That means, these are all quadratic non residue mod 11. And surprisingly the cardinality of these two set are same and this is true in fact, in the later stage we will see that even we will try to prove that this thing is true. So, a set number of quadratic residues a number of quadratic non residue where basically these are same set.

So, now we will have Euler's criteria for a quadratic residue. So, it is a condition for a to a quadratic residue.

(Refer Slide Time: 22:21)



So, let us state this is a necessary and sufficient condition. So, this is basically by Euler's that is why it is called Euler criteria; c r i, criterion for quadratic residue. This is a theorem; this theorem is telling the statement of this theorem is basically. So, let p be a prime and then say then an integer a is a quadratic residue mod p if and only if this is the condition, if and only if a to the power p minus 1 by 2 is congruent to 1 mod p. So, this is the Euler condition for a to be a quadratic residue; that means he has a square root.

So, this theorem is telling a a will be a quadratic residue; that means, a has a square root if this condition satisfied, it is in both the way if and only if so; that means, this is a necessary and sufficient condition. So, this condition will used to check whether a integer is a quadratic residue or not. So, let us try to prove this theorem. So, how to prove this theorem? There are two ways: first let us assume this is a quadratic residue. So, this is if and only if condition suppose, so first part if let us assume this is a quadratic residue then we have to show this condition is satisfying and the conversely let us have this condition then you have to show the a is a quadratic residue.

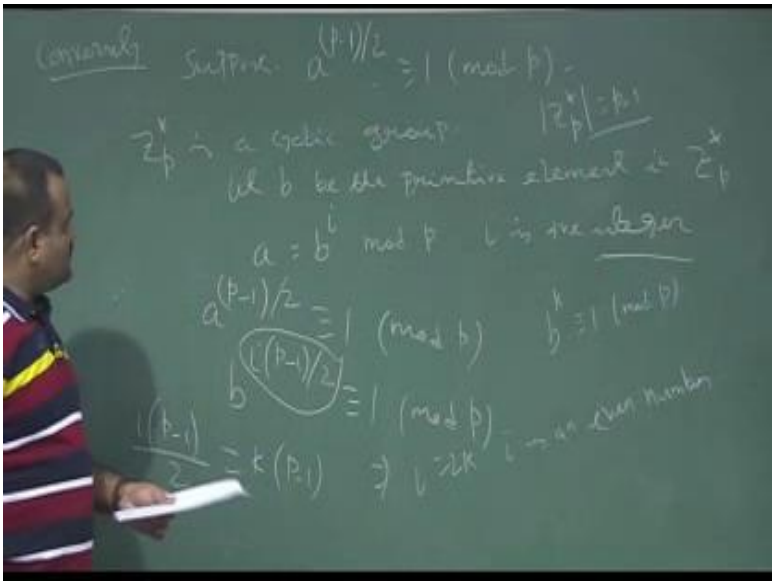
So, let us first suppose a is a quadratic residue mod p, so sorry. So, suppose a is a quadratic residue mod p then you have to prove this theorem; we have to prove this result. If a is a quadratic residue mod p, that means we have a y; that means there exists y

in Z p such that y square is congruent to a mod p. That means, we have a solution under modulus operation of p. That means there exists y such that this satisfied; and y is from Z p.

So, basically a is y square mod p. So, we have a to the power p minus 1 by 2 this is basically congruent to; a is congruent to y square mod p so we will just write y square then p minus 1 by 2, so this is basically y to the power p minus 1. Now this is what, now y is? Y is Z from Z p, so that means y is p is a prime so y must be co prime with p so; that means, by Fermat's little theorem or the Euler's theorem particular case of Euler's theorem this is coming Fermat's little theorem this is basically 1 mod p. So, this part is done, so a to the power p minus 1 by 2 is congruent to 1 mod p. This part is done.

Now the reverse, suppose this is true then we have to show a is a quadratic residue so that you have to prove now. So, now we have to prove we have to assume this condition is satisfying and then we have to show the a is a quadratic residue.

(Refer Slide Time: 27:05)



So this is the conversely, suppose the condition is satisfying. Suppose, a to the power p minus 1 by 2 is congruent to 1 mod p. Now we have to show that a is a quadratic residue; that means you have to get a y basically. So, how to get a y? Now Z p, p is a prime so Z p star is a cyclic group. So, it has a generator or the primitive element let b be the generator or the primitive element in Z p star. So, now a is a element from Z p star,

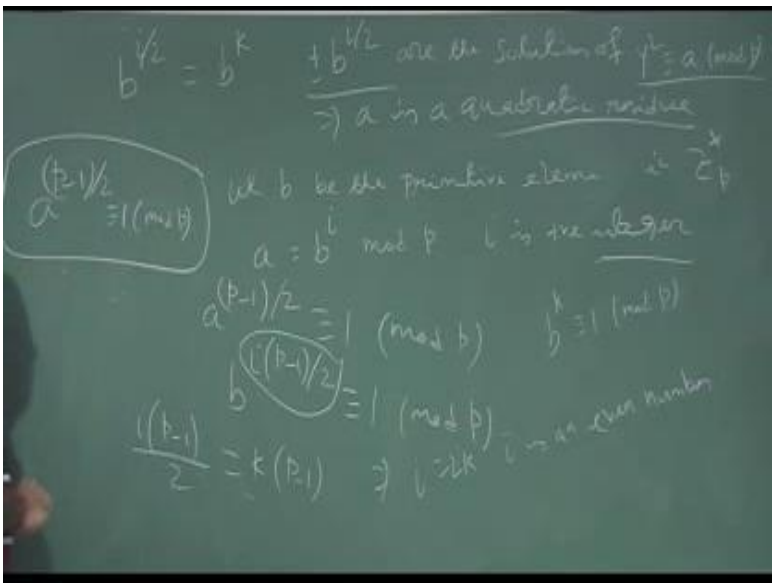
basically we are looking for quadratic residue less than p basically positive integer less than p.

So, that means a is a element, so a will be written as. So, this b must generate the group. So, a is an element, so a will be written as some b to the power i mod p for some integer for i is an primitive integers i could be 2 3 something.

So, now we will use this Euler's. So, we have this result this is 1 mod p now we will put here b, so b to the power basically i into p minus 1 by 2 1 mod p. So, b is a generator. That means, this is the order of b, order of b means the b generates the group order of b means the minimum integer such that b to the minimum integer k such that b to the power k is 1 mod p identity element basically. That means, this whole quantity, so this is giving us 1 so this whole quantity and we know that this Z p order Z p star is p minus 1. So that means, this must divides p minus 1 or p minus 1 must divides this. So, this must be a multiple of p minus 1, so that means this must be some k into p minus 1, because p minus 1 is the order of the group or the order of the element b because b is the primitive element.

So, this implies i is equal to 2 k. So, i is an even number. So, since i is an even number we can take i by 2 that means plus.

(Refer Slide Time: 30:36)



So, since i is an even number i is basically 2 k, so if we take this b to the power i by 2 this is basically b to the power k. So, basically plus minus b to the power i by 2 at the solution of this are the mod p obviously. Solution of this congruence system y square is congruent to a mod p. That means, it has a solution, so this implies a is a quadratic residue; that is it. So, this imply is the quadratic residue.

So, this is the condition to check whether a integer a is a quadratic residue or not. This condition p to the power is congruent to 1 mod p. So, this is the condition to check whether a is a quadratic residue or not. Thank you, this is the necessary and sufficient condition.

Thank you.