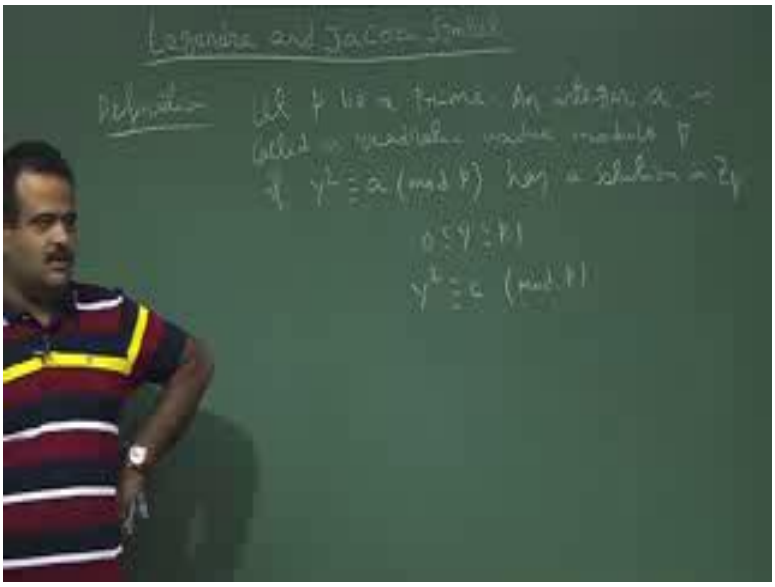
Internetwork Security
Prof. Saurav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 34
Legendre and Jacobi Symbol

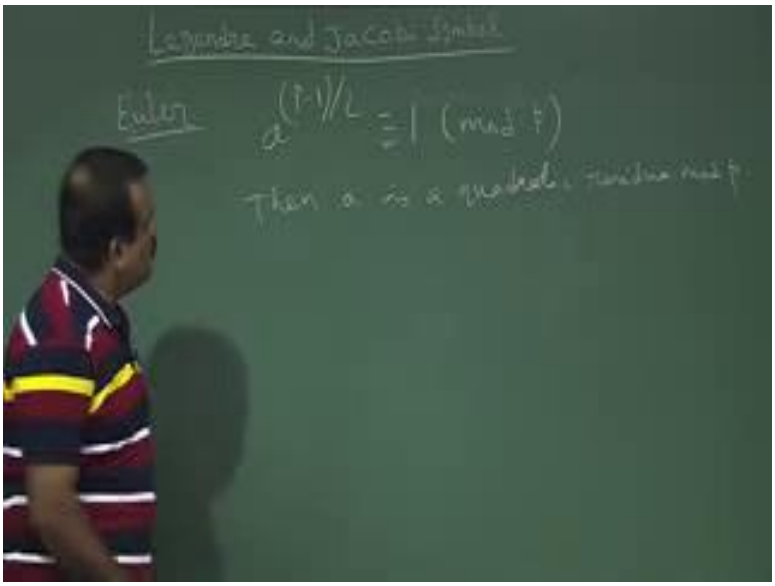
We will talk about this Legendre and Jacobi symbol which is based on what is we have see in the quadratic residue. So, let us just recap what we mean by quadratic residue.

(Refer Slide Time: 00:33)



So, this definition we have already seen. So, let p be a prime. And an integer a is called this we have seen, just to recap a called a quadratic residue modulo p if it has a square root; that means, if y square is equal to congruent to a mod p has a summation in Z p. That means, if there exist a y, 0 less than y less than equal to p minus 1 such that y square will give us a, so that means, you should able to square root that find the square root of a then it is called a Quadratic Residue. And we have seen some result on quadratic residue like by Euler's result.

(Refer Slide Time: 02:06)



So, the Euler's theorem is telling, Euler's criteria is telling if a to the power p minus 1 by 2 is congruent to 1 mod p, where p is a prime, then a is quadratic residue mod p. So, this result we have seen. So, this result we have proved.

(Refer Slide Time: 02:58)

So, now today we will talk about before defining these two symbol let us talk about how many quadratic residue and quadratic non-residue are there in the over p. So, say this is by theorem, this theorem is telling let p be a prime number. So, we are not concentrating two, so this is a odd prime. And then if we denote the Q R basically is the quadratic

residue class Q R p is denoted by Q R this is the set of quadratic residue mod p. And Q R p bar is the set of quadratic non-residue mod p. Then this theorem, we want to show that these two set are same cardinality of these two set are same. The number of quadratic residue is same as number of non-quadratic residue, cardinality of these two set are same. So, we will prove this theorem.

(Refer Slide Time: 04:43)

So, before prove this theorem, let us take the example. So, suppose p is equal to say 5. So, p is equal to five who are the quadratic residue we can easily verify that. So, for p is equal to 5, the quadratic residues are basically 1 and 4. And the quadratic non-residue are basically 2 and 3. And say for p is equal to 7, we have quadratic residue are basically 1, 2 and 4; and quadratic non-residue is 6. This can be easily verified p is equal to 11. This example we have seen 3, 1, 3, 4, 5, 9; and quadratic non-residue are basically quadratic residue minus that set z n coming here z p.

And for p is equal to 11, 13 these are the quadratic residue 1, 3, 4, 9, 10, 12 and then these are the quadratic non-residue. So, these sets are equals, so that means if we take a prime p then a number of quadratic residue over z p over this modulo p is same as number of non-quadratic residue over p.

(Refer Slide Time: 06:26)

So, how to prove this? So, to prove this we will basically this set if we consider this set 1 square, 2 square up to p minus 1 by 2 whole square mod p, so these sets will give us basically Q R p every operation is under mod p, these are basically give us the Q R p quadratic residue. So, how many numbers of elements are basically p minus 1 by 2. So, what we need to show we need to show that any two element in this set are distinct then we are done.

So, let us take two elements from this set x square so and y square. So, suppose they are not distinct; suppose x square is congruent to y square mod p, where x or y both are coming from 1 less than x less than p minus 1 by 2, 1 less than y less than or equal to p minus 1 by 2. Now, from here we can say x square minus y square is congruent to 0 mod p. So, this implies x minus y x plus y is congruent to 0 mod p. So, these imply x must be congruent to x equal to y basically, so that is the proof. So, this means if we take two distinct x y then they are not same.

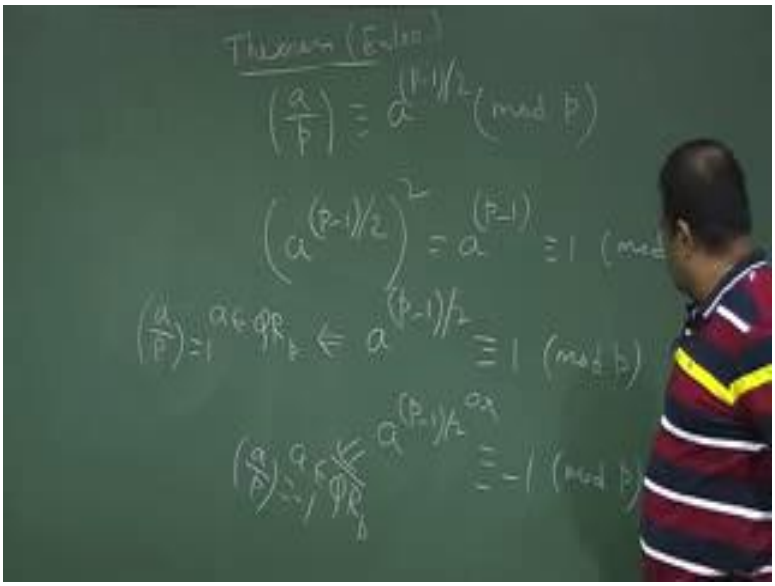
So, this completes the proof. So, the numbers of element in the quadratic residue are basically this set and then so there is p minus 1 by 2 element in this set and so the remaining elements basically are the; so Q R p bar is basically Z p star minus Q R p. So, the cardinality of this set and this set are same. So, this is the proof.

(Refer Slide Time: 09:08)

Now, we will define what is called Legendre symbol. So, Legendre symbol is basically defined as these let p be a prime; for Legendre we need p to be prime be a prime number, and a be any integer. This is definition of the Legendre symbol. Then we define a by p like this, this is the Legendre symbol, this is the symbol - Legendre symbol, this is how we denote the Legendre symbol. So, this is basically have possible three values it is 0, if a divides p, if a divides p or p divides a; and it is 1, if a is a quadratic residue mod p; and it is minus 1, if a is quadratic non-residue mod p. So, this means a is a quadratic residue mod p, this means a is a quadratic non-residue mod p. So, it can take three possible values, but we have to be careful for p this Legendre this p is prime.

So, Jacobi we will see Jacobi is the general form where p need not be a prime, p could be a any integer. So, we will see this Jacobi symbol later on, but for the time being we are talking about Legendre symbol; for that we need p must be a prime and this is defined by this functional form. So, it is 0, if a divides p. So, say if a is equal to 2 p or 3 p like this then otherwise if a is not divides p, so then it is 1 if it is quadratic residue mod p; it is minus 1, if this quadratic non-residue.

(Refer Slide Time: 11:54)



Now, we will talk about some result based on the Legendre symbol or we can say theorem. First theorem is by again by Euler, so this is the theorem again from Euler, Euler criteria. So, it is telling that if a by p is congruent to a to the power p minus 1 by 2 mod p a to the power p minus 1 by 2 this is p minus 1 by 2 mod p. So, if you have this then we can calculate this because if we can calculate this symbol because this is just the exponent.

So, now how to prove this theorem. So, to prove this theorem, so if a is congruent to 0 mod p; that means, a is a multiple of p then we know a by p is 0, and also it is easy to so that in this case a to the power p minus 1 by 2 this is also mod p this is also 0. So, when a divides p basically, so this is case one. Now, suppose case two, suppose a does not divides p. So, in this case, what we will do. So, in this case, this Jacobi symbol a Legendre symbol is either 1 or minus 1 depending on whether if this is a square root or not.

So, in this case, what we will do will take this a minus p by 2 is square it up. So, this is basically give us a to the power p minus 1. Now, this we know by the Fermat's little theorem, this is congruent to 1 mod p. So, this is case two. So, this implies either a to the power p minus 1 by 2 is congruent to 1 mod p or because this is 1, square of this is 1. So, this is either 1 or it is minus 1 mod p. Now, we know this is 1, if a is a quadratic residue. So, we know if this is 1 then a is a quadratic residue mod p. And in that case, if a is a

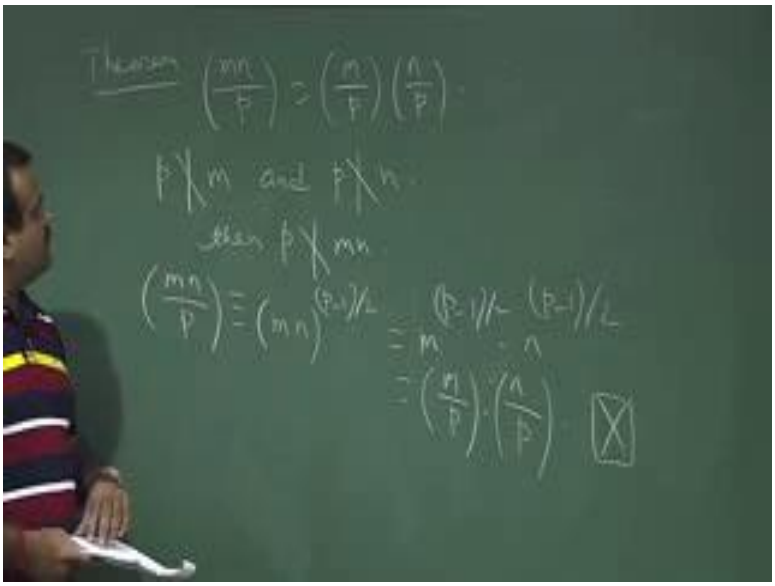
quadratic residue, then a by p we know a is one so; that means, a by p is same as a to the power this.

Now, if it is minus 1 then this implies a is quadratic non-residue mod p. And in this case it is minus 1. So, in this case, we know by definition of Legendre symbol this is minus one. So, if you combine these two and in the earlier case this is the same as; so a by p is equal to a to the power p minus 1 by 2 mod p. So, this is the theorem or this is a result. So, this result will help us to calculate this Legendre symbol of some numbers. So, this is the proof of this theorem. So, we will use this theorem to calculate this. So, let us have few more theorems on this.

(Refer Slide Time: 16:10)

So, suppose if p is prime, so m n are two integers. So, m n p is n by p, where m n are two integer or m and n are any two integer, integer like here. P is a prime here; so far we are taking p prime. This is mandatory because this is the Legendre symbol. So, how to prove that? So, to prove this, suppose p divides m n, if p divides m n this means m n by p is 0; and p divides m n means either p divides m or p divides n so that means, either m is a. So, if this is the case if p divides m; that means, m this is 0 or this is 0. So, in any case either of these two is 0, so that means, this product is 0 and we have this 0. So, this is when p divides m n.

(Refer Slide Time: 18:08)



Now if p does not divide m or n then we will use the Euler's theorem to prove this. So, suppose p does not divide m, and p does not divide n, so that means then p does not divides both m n. So, in this case, m n by p is basically we will use the earlier theorem Euler's theorem, so it is basically m n to the power p minus 1 by 2 mod p. So, this is basically m to the power p minus 1 by 2 into n to the power p minus 1 by 2. So, this is basically m by p into n by p. So, this proves this theorem. So, this is if you have product m n then it is basically product of the individual Jacobi's.

(Refer Slide Time: 19:33)

So, now another theorem which is coming the earlier from the Euler's result; so this is telling minus 1 by p is basically, so we can take this of minus 1 by p, so that means, a is minus 1 is basically; so, this is by Euler's criteria this is basically minus 1 to the power p minus 1 by 2 mod p. So, this is basically 1, if p is congruent to 1 mod 4; and it is minus 1, if p is congruent to 3 mod 4. Since p is prime, so p is either congruent to 1 mod 4 or p is congruent to 3 mod 4 either one of these, because other two option like 4 k plus 2 those are not give us p prime.

So, this is basically p is, so from here, if p is congruent to 1 mod 4 we can put this value and we will get 1; and if p is congruent to 3 mod 4, it will give us 4. So, this proof prove is also straight-forward.

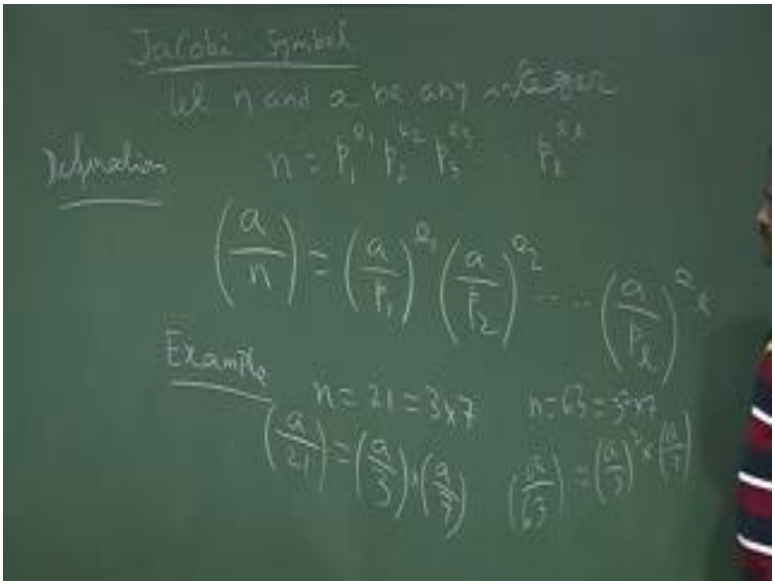
(Refer Slide Time: 21:00)

So, now the next result. So, this result will be using for calculating the Legendre symbols. So, next result is telling us 2 by p. So, 2 by p, here p is a prime because these are all Legendre symbol is minus 1 to the power p square minus 1 by 8. And this is basically 1, if p is congruent to plus minus 1 mod 8 that means p is congruent to 1 mod 8; and this minus 1 means p is congruent to 7 mod 8 or. And this is minus 1 if p is congruent to plus minus 3 mod 8 plus minus 3 mod 8, so that means, if p is congruent to 3 mod 8; and for minus 3, it is basically 5 or p is congruent to 5 mod 8. This also can be prove this theorem. So, this is basically telling us 2 by p is basically minus 1 to the power this. So,

if p is either of this form then it will be define just we can put the value of p here and we will get either 1 or minus 1 there.

So, next we will define what is called Jacobi symbol. So, it is a generalization of the Legendre symbol and so far we have assumed p is prime. Now, what happened if p is not a prime then how we define this symbol, so that is called Jacobi symbol.

(Refer Slide Time: 23:07)

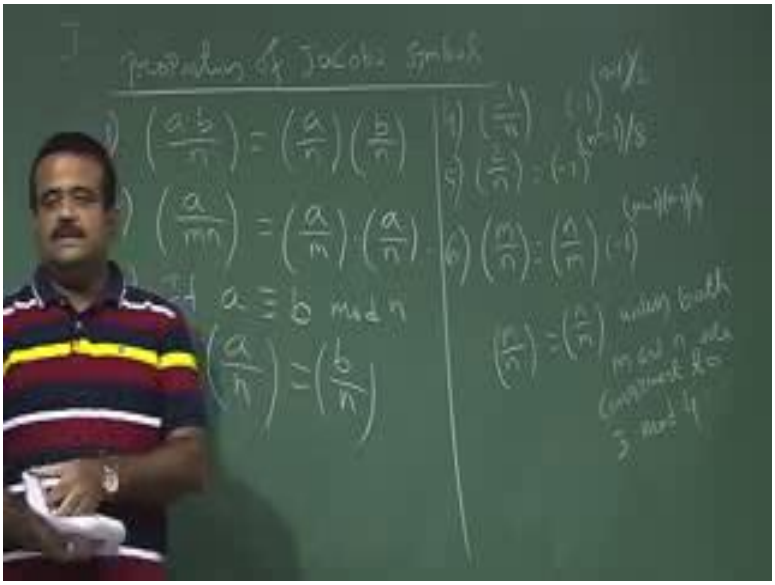


So, this is different for any integer n. So, let n and a be any integer. Now, if n is an integer. So, it is either a prime. If it is prime near the Legendre symbol; or if it is not a prime, then it must be written as the product of the prime that is the fundamental theorem of arithmetic. So, n must be written as p 1 e 1 p 2 e 2 p 3 e 3 p l e l product of prime. Then this is the definition, definition of Jacobi symbol. We define a by n is basically a by p 1 to the power e 1 a by p 2 to the power e 2 like this a by p l to the power e l. So, this is the definition of a by n, where n is not a prime.

So, for example, suppose we want to show for example, suppose we take n is equal to 21 or say 63, for it is a n, n is equal to 21 simpler one, so 3 into 7. So, 3 7s are prime now n a of a by 21 is basically defined as a by 3 into a by 7. So, now, if n is equal to say 63. So, this is basically 3 square into 7. So, a by 63 is basically defined as a by 3 square into a by 7. So, this is the Jacobi symbol is defined through the Legendre symbol. So, now, we will talk about some properties of this symbol, so that we can use this to calculate the

Jacobi's. So, these are the result on the Jacobi symbol, and this can be proved by this factorization of the primes in Legendre symbol.

(Refer Slide Time: 26:11)



So, these are the properties of Jacobi symbol. So, like this, first properties, we can write this a b by n is equal to a by n b by n. So, this can be proved on that Legendre symbol theorem we have seen this type of resulting and Legendre symbol. Now, a by m n is basically a by m into a by n. So, these also we can prove. And if a is congruent to b mod n then a by n is basically equal to b by n. So, this similar to we can do it for when n is prime that prove is coming from that Euler criteria, but this can easily proved; if a is congruent to b mod n then a by n is equal to b by n.

So, another result could be say 4, minus 1 by n this we have seen minus 1 to the power n minus 1 by 2. So, 5 is 2 by n is equal to minus 1 n square minus 1 by 8. So, now we have a reciprocal theorem. So, n by m or m by n is equal to n by m to the power minus 1 to the power m minus 1 into n minus 1 by 4. So, these are the theorem or result; this can be easily checked by using the factorization and then the Jacobi symbol. So, this is either 1 or minus 1 depending on these values. So, this is mostly m by n is equal to n by m mostly it is there unless both m and n are congruent to 3 mod 4, unless this we have these results. So, they are reciprocal.

So, we will use this result to find out the Jacobi symbols of any number a by n. And we will see how it will be useful for have a cryptosystem or for the primarily testing to check whether a number is, whether n is prime or not.

Thank you.