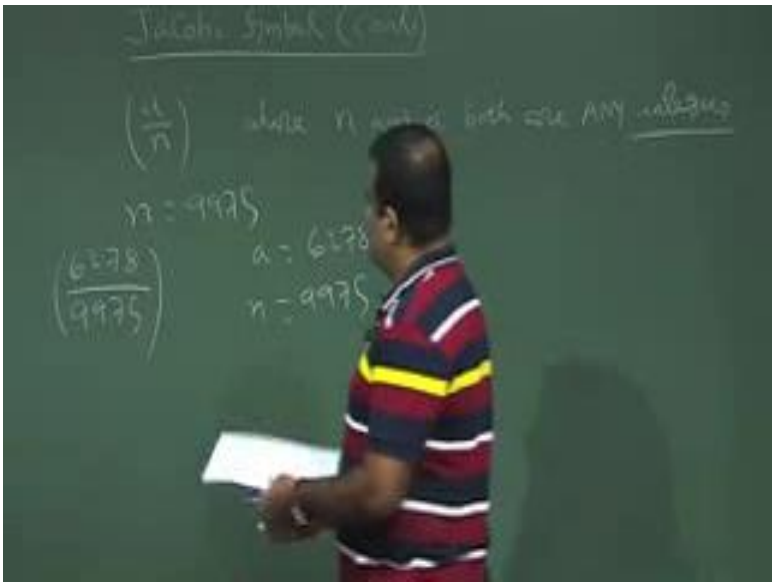
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 35
Jacobi Symbol (Contd.)

So, it is continued the Jacobi symbol. So, in the last class we have seen some of the properties of Jacobi's symbol. So, using that properties you have to calculate that a by n.

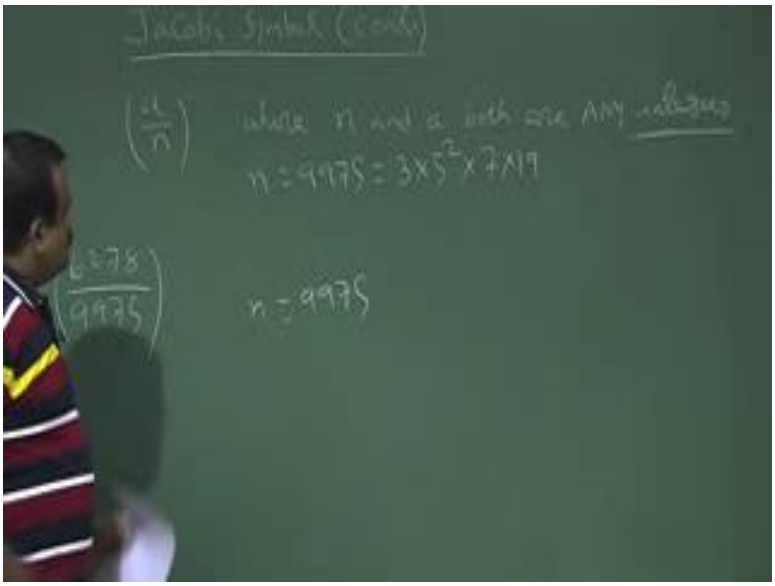
(Refer Slide Time: 00:34)



So, where a is n; a is an any integer a and n both are any integer. So, then it is Jacobi symbol.

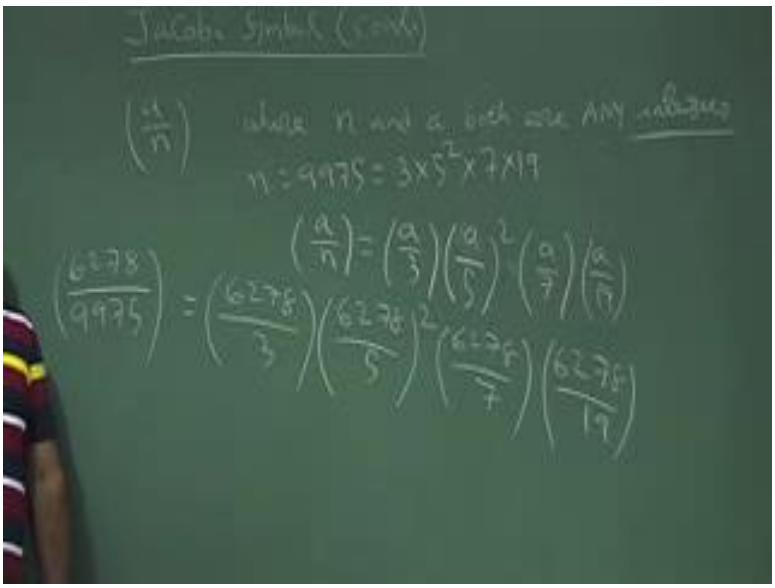
So, today in this lecture we will just talk about how we can use this to have a primary test algorithm, which is a probabilistic algorithm and also we will see cryptosystem gold or some nickel cryptosystem based on this Jacobi symbol. So, first let us have the primary test algorithm. So, before that let us just try to calculate some Jacobi's like suppose n is a 9975 and suppose you want to calculate this 6278 by 9975. So that means here a is 6278 and n is 9975.

(Refer Slide Time: 01:50)



So, we know that we have to convert this into this n has to be n should be written as a product of prime. So, n is basically if we just verify 3 into 5 square. So, this is coming from fundamental theorem of arithmetic, f e integer is either a prime or it must written as product of prime.

(Refer Slide Time: 02:18)

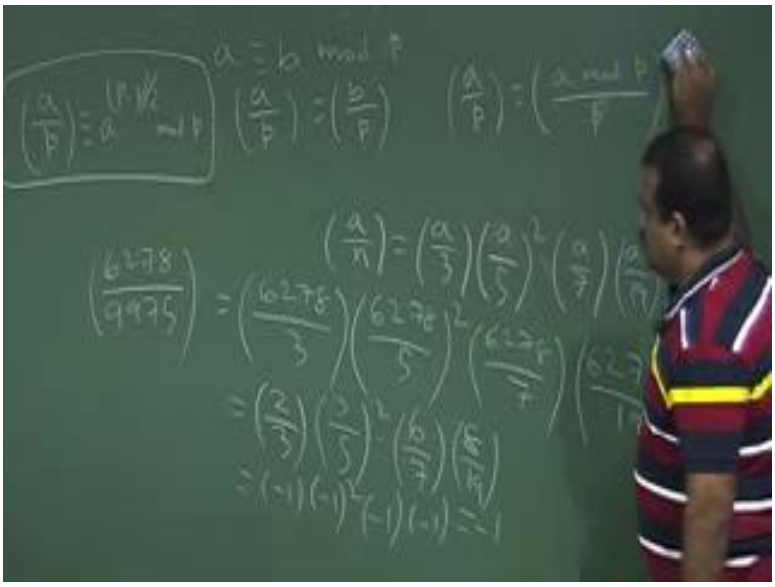


So, then if this is the n then we know the definition of this Jacobi symbol. So, basically a by n is equal to for any integer. So, which is basically a by 3 5 by sorry a by 5 square into these are all into; a by 7 a by 19.

So, this is the definition of Jacobi symbol. So, we will use this definition to calculate this. So, this is basically if we use this a is basically 6278. So, 6278 by 3 then 6278 by 5 square, into 6278 by 7 into 6278 by 19 ok.

So, now we have to use some properties of this Jacobi symbol, in the last lecture we have seen some properties. So, basically here for the time being you have to use this properties that.

(Refer Slide Time: 03:38)

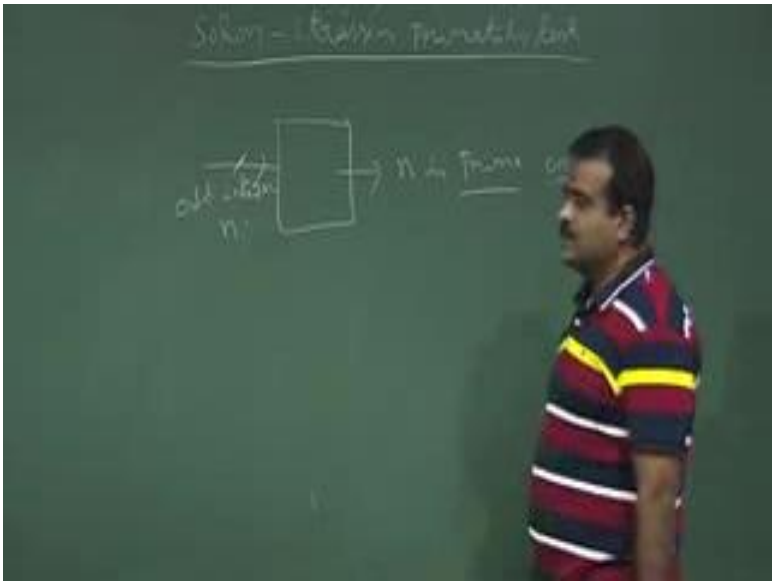


If a is congruent to b mod n, then I mean this is P. So, you can just have P, the Legendre symbol this is basically these are all basically Legendre symbol. So, then a by P is equal to b by P. So, basically we try to divide this by 3 then the so this is basically. So, a by P is equal to a mod P by P. So, we will divide this by 3 and the remainder will be the basically 2. So, this is basically 2 by 3 and if we divide this by 5, this a then this will give 3 as a remainder. So,3 by 5 square into. So, this also can be verified 6 by 7 into 8 by 9.

So, now if we. So, 2 by 3 we know the formula. So, this if we just check whether they are quadratic residue or we can apply the properties of the Jacobi symbol, you can easily check this is minus 1, this is also minus 1 square, this is minus 1, this is minus 1, this value is coming out to be minus 1. So, by this way we can calculate one can calculate this thing. So, this is also can be calculated by Eulers theorem. So, basically this is a by P; a by P is equal to congruent to a to the power P minus 1 by 2 mod P; here P is prime.

So, that is why it is anyway. So, one can calculate this. So, now, we use this Jacobi symbol to have a primary testing of a integer a or integer n.

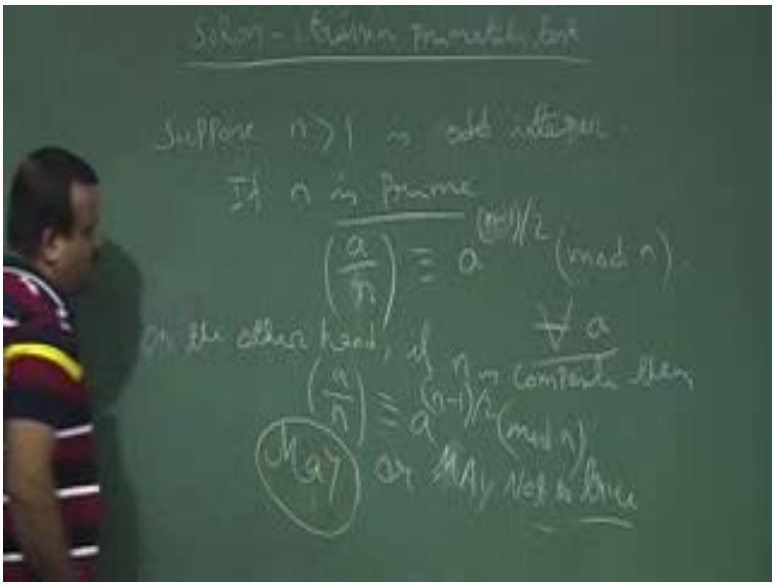
(Refer Slide Time: 06:16)



Now suppose so this is basically called Solovy-strassin primarility test, we have to test given integer name is prime or not. So, primary test means, we have seen we need prime in our crypto system like RSA another crypto system; we need to have primes to in the key generation. So, now, how to get the primes, that is a challenge? So, is there any algorithm in which we can give the input, say we need 512 bit prime, we just can you can it give us a prime of 512. So, is there such algorithm? No there is no such algorithm, which can take the input as the number of bits and can give us that many bits prime number.

On the other hand what we can do? We can take an integer odd integer because even integer cannot be a prime, we can take an odd integer n and then we can verify whether n is a prime or not. So, this we know this is the called primarity test n is prime or not. So, this is called primarity test. So, this is one of the primarity test we talked about.

(Refer Slide Time: 08:00)



So, here suppose n is greater than 1, which is odd integer is there is odd integer.

Now, we know if n is prime this is by Eulers criteria; we know if n prime then a by n this is then become legend symbol is congruent to a to the power P minus sorry P here is n, n minus 1 by 2 mod n.

So, this theorem we have seen. So, this is the legend symbol because n is prime, if n is prime we have seen this result this is by Eulers criteria and this is true for all n for all integer a. Now if n is prime then this is true; now if this is true for some integer a then we cannot say m is prime. So, on the other hand if n is composite, then this may or may not true then a by n is congruent to into the power this mod n this result, may or may not be true.

Now, if it is true, but this is for only one few a; if it is true then we can say then we call n is a pseudoprime base a, if this result is true for a given a, then we call this is true for this, this n is a pseudoprime it could be a real prime, but so far we check this is for a.

(Refer Slide Time: 10:37)

So, then if a by n is congruent to a to the power p minus 1 by 2 mod n, if such a exists and then n is called pseudoprime or Euler pseudoprime. Pseudoprime base a and if it is true for all a if n is pseudoprime base all integer a then it is a real prime.

So, for example, if we calculate this 10 by 91; so our n is 91 and a is 10. So, if you just calculate this Jacobi, you can verify this is 1 and if we calculate this 10 to the power 91 sorry 91 minus 1 by 2. So, this is basically 45. So, 45 mod 91, this also can be verified this is minus 1. So, this result is true for a is equal to 10; all the 91 is not a prime, but 91 this implies 91 is a pseudoprime based 10. If it is true for all such a then we call it is a then it will be a real prime, but n is a composite although there exist some a for which this Euler criteria is satisfied, then it is called pseudoprime.

So, based on this we have this primarity testing algorithm, which is solovy stations algorithm, which is taking an input as an integer n and it is telling us this is a probabilistic algorithm. So, it may correct may not correct with some probability, so the probability of success.

(Refer Slide Time: 13:06)

So, this is taking an integer n and it is telling us whether it is a prime or not. So, what we are doing? So, we choose a randomly a, a integer a from Z n minus 0; choose a randomly from Z n minus 0. So, a we are choosing from this is randomly for 1, 2 up to n minus1 I am not taking 0.

Now, we calculate this symbol Jacobi. So, far we should say this is a Jacobi symbol, we do not know whether n is prime or not. If n is prime then we call this is legend symbol, but we do not know yet. So, we calculate this now if x is 0 then surely we can say this is a composite then return n is composite because then a is the factor of n. So, a divides n basically; so then it is a composite number. So, n has a factor that is a now, this is 4. 5 is basically now we compute that Euler y. So, this is y is basically a to the power n minus 1 by 2 model. So, this can be calculated using this exponent exponentiation.

And now if x is congruent to y mod n, then we return n to be a prime actually this should be a pseudoprime based a, but anyway since we are choosing a randomly. So, if for random choice of a give us still as this n could be a prime. So, that is why it is a problistical algorithm. So, they may return if this is n, we return n is a prime which should be this pseudoprime actually, else if this is not true then we return n is composite that is correct. So, else we return our n is composite number.

If it is telling us it is composite, that is perfectly alright no no pseudo composite, but if it is telling it is a prime then it is a pseudoprime like if we choose that 9th one earlier

example, if we test by these algorithm n is equal to 91 and if it is happened that our random choice of a say 10, then we have seen that these two are same and these algorithm is returning this 91 is prime which is not; actually 91 is a pseudoprime base 10.

So, this is a problistical algorithm. So, it may correct may not correct, but if it is telling us n is composite then it is correct. So, this is the one application of this Jacobi symbol in my context of primary test, now next we will talk about a cryptosystem based on this Jacobi symbol. So, this is a public key cryptosystem.

(Refer Slide Time: 17:28)

This is called a Goldwasser-Micali cryptosystem; this is a public key cryptosystem. So, so little let us just sequel we have two party Alice and Bob. So, now, Alice wants to send a message to Bob and in public key. So, Alice needs to get Bob public key so; that means, Bob needs to generate box public key appear, this is the box secret key or the private key this is the box sorry this is the Bobs public key, which need to be sent to Alice in order to Alice to encrypt the message and send it to Bob and this is the secret key of Alice. So, this key is ever because Alice has to send Bob is the receiver. So, Bob has to run this setup phase or the key generation phase. So, in the setup phase, Bob is choosing, 2 prime number like P and q b two prime number.

And then Bob is computing n which is basically P into q, this is a setup test done by the receiver Bob, Bob is choosing this and then Bob is choosing a m, which is basically such that m by p is equal to minus 1 is equal to m by q so; that means, m is non quadratic

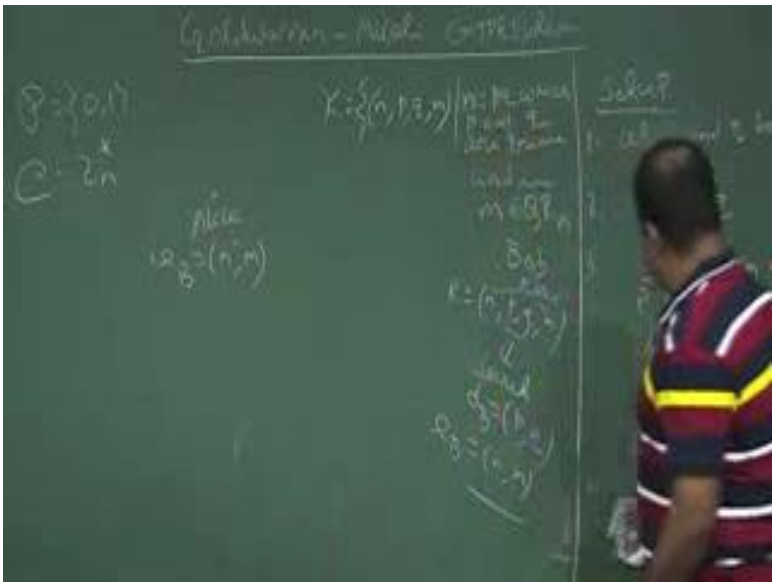
residue mod p and also non quadratic residue mod q. So, m does not belong to what. So, m is does not belongs to quadratic residue of mod p and also m does not belongs to quadratic residues of mod q. So, m is a non quadratic residue of mod p and mod q.

But by what is then m, m by n? So, m by n is then basically. So, this is m is equal to p q. So, m by n is basically m by p into m by q small m. So, this is 1. So, by saying this we may guess that input be the quality residue mod n. So, this is the quadratic residue. So, you have to depend the quantity residue mod a composite number, so just quickly we can define. So, if we have a competition number n which is a product of two primes; so any number if we either product of two primes or prime factorization. So, number a is a quadratic residue mod n if and only if it is quadratic residue in both p and q if a not this is the definition of quantity residue on a composite number, if and only a is a quadratic residue mod p and also a is a quadratic residue mod q.

So, if a is the quadratic residue both these primes, then we say because we know the definition of quadratic residue based on the prime modulo p or modulo q then we say a is a quadratic residue mod n, but by saying this definition this Jacobi symbol this could be tell us that a could be a n could be a quadratic residue model, which is not true, but it is. So, that is why it is called pseudo quadratic residue. So, that is why n is belongs to QR of n this is the set we can define as pseudo quadratic residue. So, it is not a quadratic residue although we are getting this Jacobi symbol is 1. So, this is called pseudo quadratic residue.

So, this is the setup phase, now after run the setup phase Alice so Bobs generates this key here.

(Refer Slide Time: 22:55)



So, Bobs key set is basically this is a key set n, p, q, m such that p is equal n is equal to p q as p q are prime, where p and q are prime and n is chosen to be says that, m belongs to QR n pseudo pseudoprime pseudo quadratic residue; that means, m is chosen says that m by p is equal to mine this is a Legendre symbol Legendre symbol of this value m is minus 1 Legendre symbol of value under mod q is minus 1.

So, this is the key generation. So, this is doing by Bob and so this is the one key content n, p, q and m. Now this p q r basically secret key of Bob, secret key this is d b of Bob, this is p comma q and these two basically is public key of Bob. So, e B of Bob is n comma m. So, e b of Bob is public. So, it is available to the sender which is basically Alice. Now Alice also send a message, here message space is basically 0 1. So, it is a one bit encryption basically this cryptosystem, we can encrypt this x which is (Refer Time: 24:48) 1 bit and the ciphertext space is basically Z n star and key space we know this is the key space. So, now what is the encryption? So, just erase this. So, what is the encryption? So, Alice got Bobs public key.

(Refer Slide Time: 25:17)

So, encryption will be like this. So, Alice chooses the plaintext suppose x is a plaintext from this 0 1 it is either 0 or 1. So, encryption of e B x now Alice choose a r randomly Alice is choosing r. So, this r is coming from. So, this is Alice is chosen r, randomly Alice is chosen from Z n and star.

So, the encryption of this along with r is basically m to the power x r square model. So, m is known m is one of the public parameter of l Bobs, and r Alice is choosing, an r square Alice can compute m to the power x. So, if x is 0 this is 1; if x is 1 this is m. So, this is a y. So, this y is the cipher text y sending to Bob. Now how Bob will get back the message? Now that is the decryption phase, now how to decrypt it? So, Bob is having his secret key which is basically p q. So, Bob has to check. So, if y is a quadratic residue mod n, then it is basically then x must be 0 because this is just must be r square. So, the decryption is like this the decryption of D v on y is basically. So, it was 0 if y is a quadratic residue mod n it is 1, if y is quadratic non residue.

So, Bob has to check whether y is a quadratic residue model or y is a quadratic non residue model; so to check that because if x is 1 then this is n. So, this cannot be the square of something. So to check that what Bob can do, so Bob has to calculate this number. So, y by p Bob can check this whether this is p minus 1 by 2 sorry Bob can check this mod p. So, then and also Bob has to check y by q is congruent to y to the power q minus 1 by 2 mod q. If any one of these not satisfying then Bob can easily say y

is not a quadratic residue; that means, corresponding x is 1, otherwise corresponding x is if we both the case both the it is satisfied then, why this quadratic residue mod m then we say that then Bob will recover x as a as 0.

So, this is the algorithm, which is based on the Jacobi symbol which is called Goldwasser-Micali algorithm. So, this is a problistical algorithm.

Thank you.