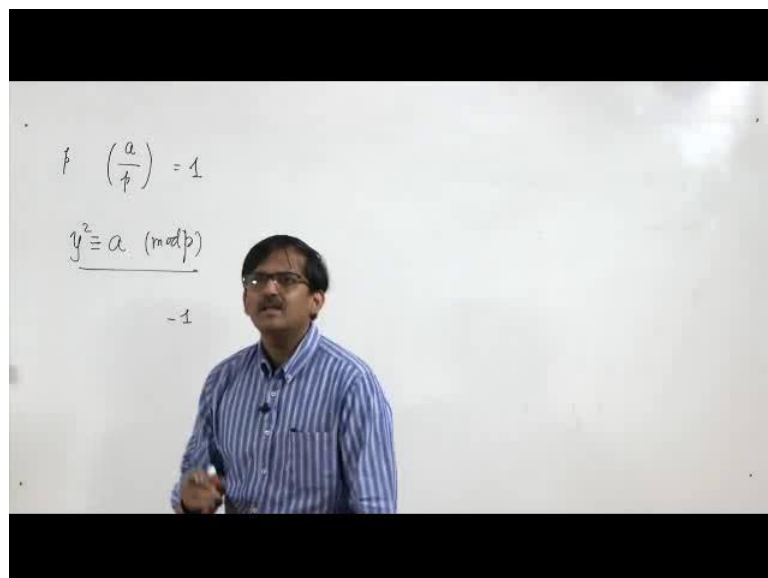


Introduction to Cryptology
Dr. Sugata Gangopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Roorkee

Lecture – 14
Efficient Computation of Jacobi symbol, Primality
Testing: Solovay-Strassen Algorithm

Hello, welcome to the 4th lecture of the third week. In this lecture, we continue our discussion on computation of Jacobi symbol that we started in the last lecture leading up to the Solovay-Strassen algorithm, which uses Jacobi symbols. Now, let us recall that, we talked about Legendre symbols.

(Refer Slide Time: 01:03)



So, for Legendre symbols, we need to have an odd prime p and then we say that a by p is quadratic residue mod p , if well the congruence equation y square equal to a mod p as a solution. And then, the value of a by p is given as 1. So, I write over here the value is missing, it is here; it is 1. If it is quadratic residue, it is 1 and otherwise it is minus 1, if it is quadratic non residue. And, if a is $0 \pmod{p}$; then, it is 0. This is what we have studied. And, we have also studied Jacobi symbol; for that, first we need an odd positive integer n .

(Refer Slide Time: 02:16)

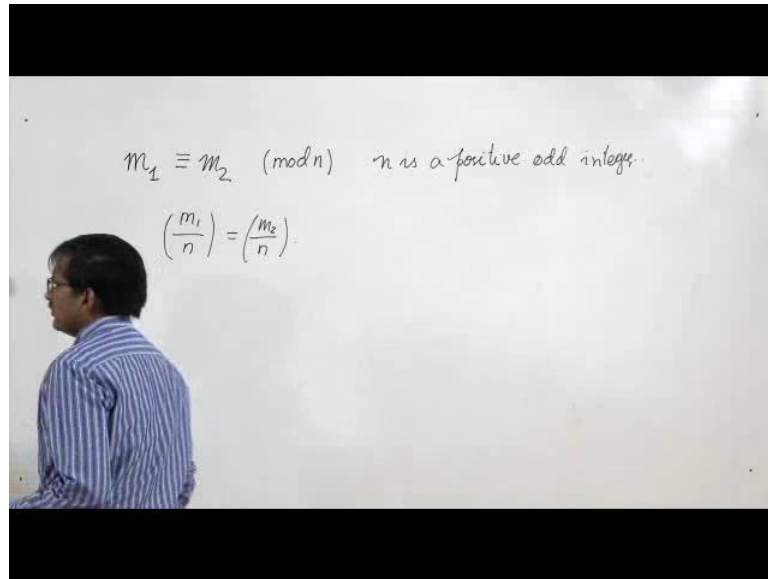
$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$
$$\left(\frac{a}{n}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{e_i}$$

p_i 's are distinct primes.
 $e_i \geq 0 \quad e_i \in \mathbb{Z}$

We factorized that integer like this; where, p_i are distinct primes and e_i 's are integers greater than equal to 1. We do this and then a by n say Jacobi symbol, is the product of Legendre symbols of a with respect to each p_i raised to the power e_i ; where, i varies from 1 to k ; all right. We have also studied the computation a technique of Jacobi symbol, which involved factorization of n . So, we have seen this calculation in the previous lecture. Now, factorizing a large number is not easy.

he question is that, can we get the same information without factorizing. And, that is what we are going to discuss today. In order to do that, we will study some properties of Jacobi symbols. And, in these lectures, we will not be able to prove them, but we have to remember them and they are not very difficult to remember. In fact, if you look at the first property, it is rather reasonable and we have also talked about this property in the last lecture when we were studying Legendre symbols.

(Refer Slide Time: 05:19)



So, it is like that, if our starting point n is an odd positive integer; then, if there are two integers m_1 and m_2 , which are congruent to each other mod n – m_1 and m_2 are congruent to each other mod n ; n is a positive – n is an odd, let me write like this n is a positive odd integer now. Then, the Jacobi symbol $m_1, m_1 n$ is equal to Jacobi symbol $m_2 n$. This is reasonable. The next property is interesting. And, it let us deal with we will let us deal with even positive integers.

(Refer Slide Time: 06:45)

Efficient Computation of Jacobi Symbols

- If n is a positive odd integer and $m_1 \equiv m_2 \pmod{n}$, then
$$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right).$$
- If n is a positive odd integer, then
$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8} \\ -1 & \text{if } n \equiv \pm 3 \pmod{8} \end{cases}$$

IT 8008EE NPTEL ONLINE CERTIFICATION COURSE 5

So, if we have two upstairs. Then, 2 by n, that is, the Jacobi symbol of 2 modulo n is going to be 1. If n is plus or minus 1 mod 8; and, is going to be minus 1 if n is plus or minus 3 mod 8. This is very useful; we must remember this. Now, let us look at the other properties. We come here. Now, this involves product in the numerator. See if have a product of two positive integers: m 1 and m 2 in the numerator; then, the Jacobi symbol will split up into products.

(Refer Slide Time: 07:39)

Efficient Computation of Jacobi Symbols

- If n is a positive odd integer, then

$$\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right) \left(\frac{m_2}{n}\right).$$
- In particular, if $m = 2^k t$ and t is odd, then

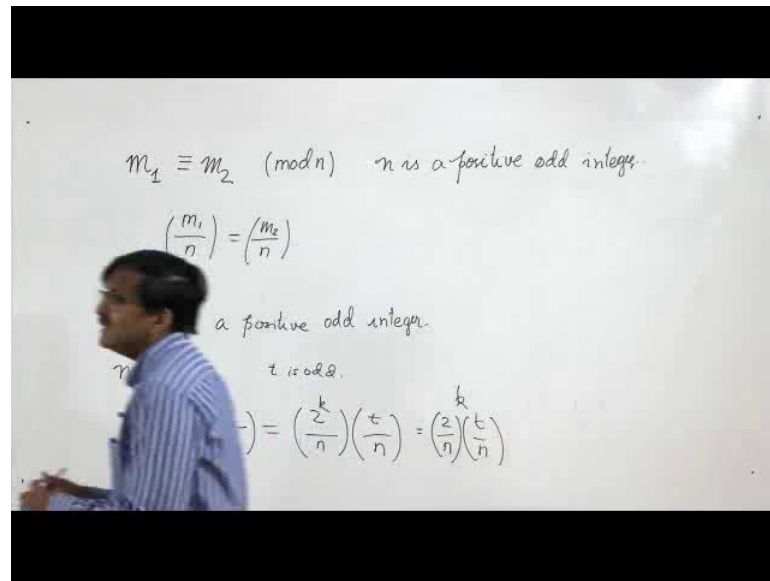
$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right).$$
- Suppose m and n are positive odd integers. Then

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{if } m \equiv n \equiv 3 \pmod{4} \\ \left(\frac{n}{m}\right) & \text{otherwise.} \end{cases}$$

IT FOOTRE | NPTEL ONLINE CERTIFICATION COURSE | 6

So, we see that, m 1 into m 2 Jacobi symbol value modulo n is product of the individual Jacobi symbol values mod n of m 1 and m 2. This is very interesting. And, we can apply this over and over again when m is 2 to the power t – 2 to the power k into t and get this. Let me explain this a little more. This is something that we have very often.

(Refer Slide Time: 08:15)



So, suppose we know that n , that is, something that is going to be in my denominator, is a positive odd integer. Now, the integer m , which is on the numerator it need not be odd; it may be even. Now, if it is even, then I can repeatedly divide it by 2 till the other factor is odd. So, that is what we will do. Let us say it is t – do its t ; t is odd. Now, then, our property tells that, if you have got m by n , this is 2 to the power k into t divided by n .

This is equal to, by using the property at the top equal to 2 to the power k divided by n ; then, it is t by n . And, this is going to be $2^k n$ raised to the power k t by n . Now, this first factor can be determined very quickly by using the second property that we discussed in the previous slide, that is, the Jacobi symbol of 2 modulo n is 1 or minus 1 depending on whether n is congruent to plus minus 1 mod 8 or plus minus 1 mod 3. So, we can take care of this part in that way.

And, the last property from the most important property in this sequence of properties is a kind of reciprocity property, which says that, if you have m by n and both are positive odd integers; then, you can tan them around; you can have m as a denominator and m as the numerator of the Jacobi symbol. And, this multiplied by sign and that sign is determined by the fact whether m is congruent to n is congruent to mod 3 – congruent to 3 mod 4.

So, here if m is congruent to n , which in turn is congruent to 3 mod 4; if it happens, then this switch over will happen with a minus sign; otherwise, there is no sign, it just

So, I have got twelve here and 175 in the denominator enclosed by a parenthesis. And, this is equal to; so, what I have to do is that, I have to check whether the numerator integer is even or odd. If it is odd, I do not have to do anything. If it is even, then I just have to take out all the possible 2 – the factors 2. If I do that, then I see I can always do that very easily. So, if I can do that, I just keep on dividing by 2 and count the number of times I have divided by 2.

And, in case of 12, it is two times I can divide by 2 and I will have the other odd factor to be 3. And, I have 175 over here; all right. And now, I can use the third property, which let me factor out the symbols. So, I will get something like this – 2 square by 17 – 175 and 3 by 175. I have got this. I can do something further on; I can take 2 by 175 and square, and 3 by 175. And now, I have to determine the sign of this thing. Although I know that, in this case, I do not have to do anything, because it is either plus 1 or minus 1. And, you know in any case, it is going to be 1, because after all, it is squared. But, still it is good to check once. So, in order to check whether 2 by 175 is plus 1 or minus 1, I have to divide n, that is, 175 by 8 and check the remainder.

Let us do that. So, 8 dividing 175 – 8 2's are 16; and then, you see that you get 1 here 15. And, I will write a little non-standard way and write again 2 over here. So, it is 16. So, if I subtract I get minus 1. So, my remainder is minus 1. This basically means this basically means that, n, that is, 175 – 175 is here is equal to 22 times 8 minus 1. Of course, this is true.

And, this means that, it is congruent to minus 1 mod 8. So, therefore, in my case, it is 17 n is equal to 175 and it is minus 1 mod 8. And therefore, I know that, it is going to be 12 by n is going to be 1 according to that rule. Now, so, it is 1. Now, I come to 3 by 175 Jacobi symbol. And, here I will be using the reciprocity law that is given at the end. In order to do that, I have to check whether in order to do that, I have to check whether m congruent to n congruent to 3 mod 4 or not; where, m and n are 3 and 175. So, I have got 4 over here and 175 over here.

So, I have got 4 4's are 16. And, I have got 5 over here. So, now, I write 3 4's are 12. So, it is 3. And, if I divide 3 by 4; of course, trivially it is equal to 3. Therefore, I have got; well, let me write over here 175 is congruent to 3 – is congruent to 3 mod 4. And, I am writing 3 twice, because I am just putting n and m over here; I mean just like this pattern.

So, we have got this. And therefore, I know you will have a switch over, but we will have to put a minus sign. So, let me remove this calculation from the board and continue this chain.

(Refer Slide Time: 18:25)

$$\left(\frac{12}{175}\right) = \left(\frac{2^2 \cdot 3}{175}\right) = \left(\frac{2^2}{175}\right) \left(\frac{3}{175}\right) = \left(\frac{2}{175}\right)^2 \left(\frac{3}{175}\right)$$

$$= \left(\frac{3}{175}\right) = -\left(\frac{175}{3}\right) = -\left(\frac{1}{3}\right)$$

$8 \overline{) 175} \begin{array}{r} 22 \\ 16 \\ \hline 15 \\ 16 \\ \hline <-1 \end{array}$
 $5 = (22 \times 8) - 1 \equiv -1 \pmod{8}$

$3 \overline{) 175} \begin{array}{r} 58 \\ 15 \\ \hline 25 \\ 24 \\ \hline 1 \end{array}$
 $175 \pmod{3} = 1$

So, I have got 3 by 175. I know that, I have to put a minus sign and put 175 by 3; all right. I have got this one and 175 is odd. So, no question of dividing by 2, so I can just go for the first law over here, which tells me to reduce modulo the denominator. I reduce modulo denominator; if I do that, let us see what happens. So, let us do the calculation over here. I have got 175 and I divide by 3; then I have got 15 over here; this is 2 and 5; 3 8's are 25 – 24. So, I have got 1.

Therefore, I can say that, $175 \pmod{3}$ is equal to 1. And, that is what I will replace over here. This is minus 1 – 1 3 and of course, 1 is a quadratic residue mod 3. And therefore, it is 1. So, I get the value minus 1. So, if we go back few steps here, here also we got minus 1 and we have got minus 1 over here. What is a difference? The difference is that, in this calculation, I needed the factorization of 175 and I do not need it in whatever I have done afterwards by using the properties of Jacobi symbol.

(Refer Slide Time: 20:34)

Solovay-Strassen Algorithm

```
SOLOVAY-STRASSEN(n)
Choose a random integer a such that 1 ≤ a ≤ n - 1
x ← (a/n)
if x = 0
    then return ("n is composite")
y ← a(n-1)/2 (mod n)
if x ≡ y (mod n)
    then return("n is prime")
else return("n is composite")
```

IT ROORKEE | NPTEL ONLINE CERTIFICATION COURSE

Now, we come to Solovay-Strassen algorithm, and let us go stepwise first and then we will try to understand or try to get a feeling that why it works; all right. So, looking at a Solovay-Strassen algorithm, you will see that, the input is n. And, just as before, there is no point checking with n even, because after all, an even positive integer cannot be a prime. So, we will take a positive odd integer n as a input.

(Refer Slide Time: 21:34)

n is a positive odd integer.
 $1 \leq a \leq n-1$
 $x \leftarrow \left(\frac{a}{n}\right)$
 $y \leftarrow a^{\frac{n-1}{2}} \pmod{n}$

p
 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$
 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$
 $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$

And, after doing that, we will choose an integer a; let me first write n is a positive odd integer; all right. And, we choose an integer between 1 and n minus 1 at random. This is

also something very important and that is often not realise – not I mean that, often it will do not realise when studying for the first time that, it is a very crucial matter how to choose an integer at random between 1 and $n - 1$. But, we are not going to discuss that. So, let us suppose we are able to choose (Refer Time: 22:33), choose an integer at random and then we calculate the Jacobi symbol of a modulo n and store it in x . So, a is something, which is chosen at random between 1 and $n - 1$ and then we compute a Jacobi symbol x ; we do it.

Now, if for some reason, this symbol is 0, it is possible because if you go back to the definition of Legendre symbol, you will see that, yes, Legendre symbol can be 0; it happens if a is $0 \pmod p$. And so, if one of the factors is basically if one of the when you are factoring it out, it is possible that, one of the Legendre symbol is 0. Then, the whole Jacobi symbol will be 0. And, if it happens like that; then, we will say that, n is composite. So, we stop the algorithm. We know that it is composite.

But, suppose it does not happen; if it does not happen; then, basically, what we are doing is that, we are taking n as if n is a prime number. And, we are taking $n - 1$ by 2 calculating that and raising a to the power that quantity. And, how to do that is again a question that, how are we going to do a raised to the power $n - 1$ by 2 modulo n , if n is very large.

And, that is something that we have done in one of our previous lectures; that we can use square and multiply algorithm; we can do the square and multiply algorithm and do that. So, if we do that, then we get a value of y . So, we get y as a raised to the power $n - 1$ by 2 mod n . Compute that. And then, in the next step, we have to compare x and y . If we see that, x and y are equal, that is, to say if x is congruent to $y \pmod n$; then, we will say that, n is prime; else, we will return as n is composite. And, that is an algorithm.

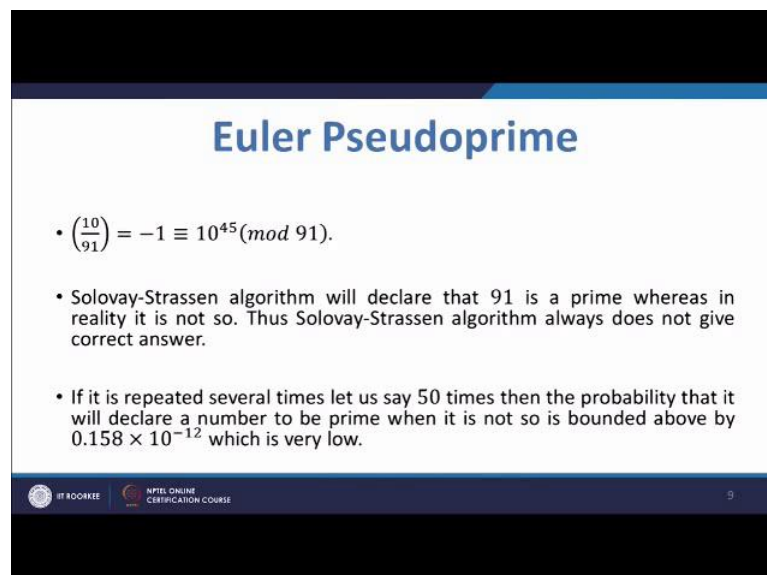
Now, the question is that, why it works. It works because we are essentially using Euler's criterion, which says that, if p is an odd prime; then, a is quadratic residue modulo p , if a is congruent to $1 \pmod p$. And, it also can be proved that, otherwise, a raised to the power $p - 1$ will be congruent to $-1 \pmod p$. So, if a is not congruent to $0 \pmod p$; and p is an odd prime; then, the Legendre symbol a by p is essentially equal to this mod p .

So, if you take a raised to the power p minus 1 by 2 and reduce its mod p , we are going to get the Legendre symbol. So, this happens if it is p . So, suppose that, n is a prime; then, whatever number I choose between 1 and n minus 1, this condition is going to be satisfied. And, if n is a prime; if instead of taking Legendre symbol, if I compute the Jacobi symbol, I am going to get the same result.

So, here when I am calculating the Jacobi symbol; if n is already a prime, it will be same as just one Legendre symbol corresponding to that prime. I am going to get some x . And, it is not going to be 0. And then, we are calculating this, which is essentially Euler's criterion and we are checking that, whether they match. If they match, they will match if n is a prime. Then of course, we come to the end of the algorithm. It says that is prime.

Otherwise, if it does not match, I know for definite that, it is composite, because if n were a prime; then, this has to be satisfied; otherwise, composite. But, interestingly, there are pairs of positive odd integers and such that the Jacobi symbol somehow works in such a way that, this condition is satisfied although the odd integer is not a prime. There are cases like that. And, in such cases, we will say that, that integer is an Euler pseudoprime. So, we will check such an integer in the next slide.

(Refer Slide Time: 29:35)



Euler Pseudoprime

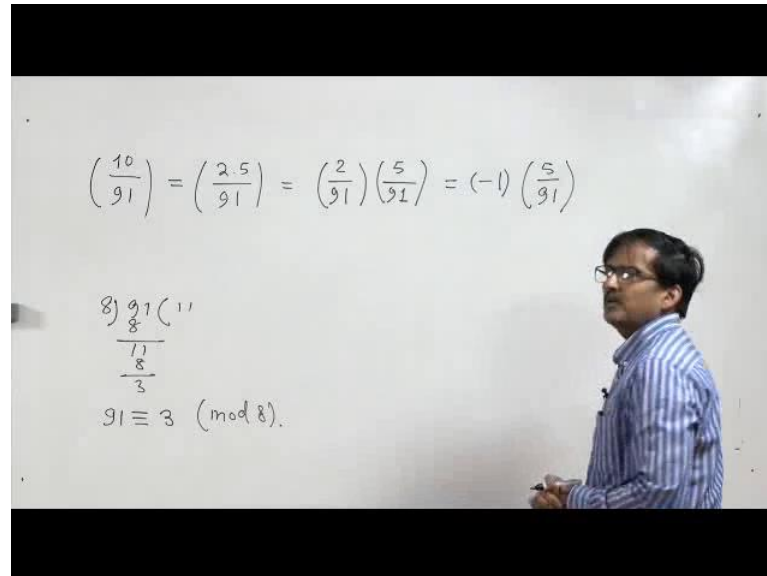
- $\left(\frac{10}{91}\right) = -1 \equiv 10^{45} \pmod{91}$.
- Solovay-Strassen algorithm will declare that 91 is a prime whereas in reality it is not so. Thus Solovay-Strassen algorithm always does not give correct answer.
- If it is repeated several times let us say 50 times then the probability that it will declare a number to be prime when it is not so is bounded above by 0.158×10^{-12} which is very low.

IT ROORKEE NPTEL ONLINE CERTIFICATION COURSE 9

So, Euler pseudoprimes; so, here let us suppose the odd integer that we are wanting to check for primality is 91. I know that 91 is not a prime. But, anyway suppose we are checking and suppose we are using Solovay-Strassen algorithm, which we have seen just

before this; all right. So, what we do? The first thing that we should do is to calculate the Jacobi symbol. Let us try to calculate the Jacobi symbol; all right.

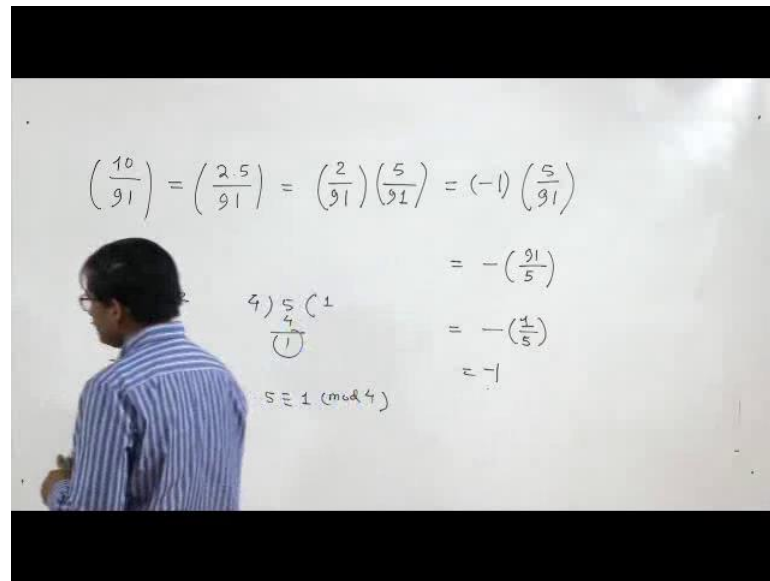
(Refer Slide Time: 30:37)



So, I have got 10 91. Now, in order to calculate the symbol, let me go back to the rules. So, I have listed the rules over here. So, let us look at these rules. So, 10 91; I want to calculate the Jacobi symbol and I do not want to factorize, because if I am able to factorize; then, I am able to know for sure whether 91 is a prime or not. But, I am not allowed to factorize. So, I come to the second rule, because 10 is a positive even integer. So, I will write this in this way – 2 into 5 by 91. And then, I use the third rule to split up the symbol. So, I get this.

Now, I should be able to know what is 2 by 91 by using the first law. So, for that, I have to divide 91 by 8. If I do that; and then 3 so we see that, 91 is congruent to 3 mod 8. Because of this, the second line will be valid. So, I know that, the Jacobi symbol of 2 modulo n is minus 1. So, I will write it over here. And then, I have got 5 by 91. And now, 5 is an odd integer. Therefore, I will go for the reciprocity. In order to check the reciprocity, I have to again do some modulo reductions. So, let us do that.

(Refer Slide Time: 33:08)



So, what I have to do is that, first I have to divide 91 by 4. So, 4 dividing 91; this is 3. And then, I have to divide 5 by 4 – 1. So, in one case, we see that, the remainder is 3. So, that means that, 91 is congruent to 3 mod 4; and, the remainder in this case is 1; that means that, 5 is congruent to 1 mod 4. Therefore, we come to the otherwise case here. So, that means I can switch over without doing anything. I switch over without doing anything. So, got minus 91 by 5; and then, I am allowed to reduce 91 modulo 5. If I do that, I am going to get 1 by 5, because of course, 90 is divisible by 5.

And therefore, and of course, 1 is a quadratic residue mod 5. So, therefore, it is minus 1. So, I come to minus 1. So, let us now jump few slides and come to the place, where place of our discussion. We see that, the Jacobi symbol of 10 modulo 91 is minus 1. So, this is what we will check over here in the algorithm when we go stepwise of this question whether this minus 1 is 0 or not. And of course, minus 1 is not 0. So, I come to the loop. Before the loop, I calculate this y; and, that is exponentiation. So, here let me remove this portion from the board. I will keep it over here.

(Refer Slide Time: 35:30)

$$\begin{aligned} \left(\frac{10}{91}\right) &= \left(\frac{2 \cdot 5}{91}\right) = \left(\frac{2}{91}\right) \left(\frac{5}{91}\right) = (-1) \left(\frac{5}{91}\right) \\ &= -\left(\frac{91}{5}\right) \\ \left(\frac{10}{91}\right)^{\frac{91-1}{2}} &= \left(\frac{10}{91}\right)^{45} \pmod{91} = -\left(\frac{1}{5}\right) \\ &= -1 \end{aligned}$$

$$\frac{13}{7} = 7 \times 13$$

So, as I get it here; so, I will have a, that is, 10 here. And, the number concerned is 91; so, 91 minus 1 divided by 2. This is 10 raised to the power 45. And, I have to reduce modulo 91. Well, I will leave it as an exercise; we can check it with a calculator after the class that, it is going to be minus 1; it is going to be minus 1 if you reduce modulo 91. And therefore, in this step of the algorithm, we will find that, whatever we have calculated as x and whatever we have calculated as y, are going to be congruent to each other modulo 91.

And therefore, the algorithm will return n is prime, which is not so, because we know that 91. So, if you take 13 into 7, it gives you 91. So, 91 is equal to 13 or rather start from the smaller integer. So, it is 7 into 13. So, it is not a prime number. But, there is a chance that, Solovay-Strassen algorithm – if the random number that we have got is a, is 10; then, it will return prime. So, we said that, the algorithm works.

And now, after this example, one would like to ask that, why the algorithm works. And, the answer is this last line – what has been found by theoretical studies is that, the error of Solovay-Strassen algorithm is bounded above. So, each time it makes an error. And if you are running this algorithm several times, we define choices of a, because a is randomised. That probability works out to be very very small.

So, what we say is that, that if it is; so, I am giving just one specific value, which makes it clear; that it says that, if Solovay-Strassen algorithm is repeated several times let us say

50 times; then, the probability that it will declare a number to be prime when it is not, is bounded above by 0.158×10^{-12} , which is a very small number. So, if you are trying with 91. If you run it few times, you will see that, you will get it will show that, 91 is not a prime. Just ones it may make an error. So, that is the end of today's lecture.

Thank you.