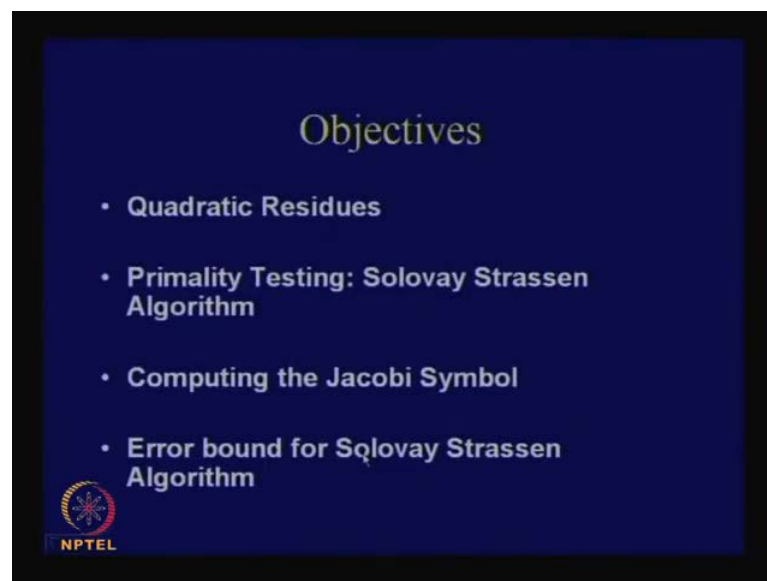


Cryptography and Network Security
Prof. D. Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Module No. # 01
Lecture No. # 29
Primality Testing

So, we will today discuss about Primality Testing algorithm. So, we are essentially continuing with the adhesive crypto system. And last time, we have actually motivated the fact, **why we are** why we would study a primality testing algorithm, because we have to choose large prime numbers.

(Refer Slide Time: 00:33)



So, therefore, what we do is that we randomly choose two numbers say p and q , and those two numbers has to be prime. So, therefore, we need an algorithm through which you would able to understand whether a number is prime or not.

So, therefore, we are continuing with quadratic residues. So, I will continue with that and then discuss about a primality testing algorithm, it is called Solovay Strassen algorithm and then there is a symbol with which we need to compute; in order to do this, I mean

have to or use this, algorithm that is called the Jacobi symbol. So, we will see how to compute the Jacobi symbol efficiently and then discuss about some error bounds for the solovay strassen algorithm, so this more or less the agenda for today.

(Refer Slide Time: 01:14)

The slide is titled "The Quadratic Residue Problem" in a serif font. Below the title, it states "(Euler's Criterion) Let p be an odd prime. Then a is a quadratic residue modulo p if and only if" followed by the equation $a^{(p-1)/2} \equiv 1 \pmod{p}$. Below this, there are two bullet points: "The time complexity of this check is $O(\log p)^3$ by applying square and multiply method to raise an element to a power." and "Note that if $a^{(p-1)/2} \equiv -1 \pmod{p}$ then a is a non-quadratic residue." In the bottom left corner, there is a circular logo with a star and the text "NPTEL" below it.

So, this is the recap of what we are studying like last time, we saw the proof of this result which is over Euler's criteria that given a number a or rather a variable a , which is a quadratic residue modulo p if and only if, a to the power of p minus 1 by 2 is congruent to 1 modulo p . So, we prove this result and therefore, if this result is satisfied then a is said to be a quadratic residue, right.

If a to the power of p minus 1 by 2 is something else then this that this not equal to 1 mod p , then a is said to be a non-quadratic residue, but the thing is that, a to the power of p minus 1 by 2 can have only 2 possible values, it can be either plus 1 or it can be minus 1 why, because this follows from the Fermat's theorem. So, Fermat's little theorem is a to the power of p minus 1 has to be congruent to 1 modulo p right, so that means that if I... So, therefore, this result is the square of one. So, therefore, it is either square root of 1, so it is either plus 1 or minus 1.

So, what we have discussed last day is that, if this is equal to plus 1 or rather this congruent to plus 1 that it is a quadratic residue, but modulo p , but if it is therefore, if it

is other way wrong that is if is the other case, it is congruent to minus 1 modulo p then a is said to be the non-quadratic residue.

So, this is the quite an efficient check because you can easily understand that we can actually do $O(\log p)$ cube, $O(\log p)$ whole cube number of steps to understand whether a number is quadratic residue or not. Otherwise, what was the newer approach, you would have continued and found out whether there is a satisfaction on the equation of x^2 equal to a, so that is not sufficient. So, therefore, this Euler's criteria use an efficient way to solve the quadratic residue problem.

(Refer Slide Time: 03:09)


Legendre Symbol

Suppose p is an odd prime. For any integer a , define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Suppose p is an odd prime. Then

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

 NPTEL

So, now we introduce a symbol which is called the Legendre symbol which is defined like this. So, this notation is like this; that is it is like within first brackets you write a and you write p like this (Refer Slide Time: 03:13). So, this Legendre symbol a comma p is actually defined like this. So, you see that its 0, if a is congruent to 0 modulo p and other ways it is, if it is a quadratic residue modulo p, then it is called 1 plus 1 and if it is a non-quadratic residue modulo p it is actually minus 1. So, these are definition of the Legendre symbol.

So, you can easily see from this definition Legendre symbol is nothing but, a to the power of p minus 1 by 2, why? Because we know that also the right hand side if a is a

quadratic residue is plus 1, if it is non-quadratic residue it is minus 1 and if a is congruent to 0 modulo p then the right hand side computes to 0, **right**.

So, therefore, you see that this and this satisfies each other and therefore, we can say that the Legendre symbol $\left(\frac{a}{p}\right)$, where p is an odd prime. So, p is an odd prime means primes which are greater than 2, then the Legendre symbol is defined as $\left(\frac{a}{p}\right)$ like this **sorry** I called it Legendre symbol $\left(\frac{a}{p}\right)$ and that is actually congruent to $a^{\frac{p-1}{2}}$ modulo p . So, these are definitions. So, it follows from the definition straight away.

(Refer Slide time: 04:39)

Jacobi Symbol

Suppose n is an odd positive integer, and the prime power factorization of n is

$$n = \prod_{i=1}^k p_i^{e_i}.$$

Let a be an integer. The *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined to be

$$\left(\frac{a}{n}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{e_i}.$$

Total Security Technology Institute
Version: 10.00
Date: 03 Nov 2008

NPTEL

So, now the next question is whatever means that is another notation called the Jacobi symbol, which actually uses the Legendre symbol. So, you will see that the Jacobi symbol is like this (Refer Slide Time: 04:50), like suppose n is an odd positive integer and the prime power factorization of n is like this. So, you see that this follows from the fundamental of arithmetic that I can take any n and I can break it up or factor it up as a product of primes **right**. So, therefore, you see that p_1 to the power of e_1 , p_2 to the power of e_2 and so on, right. So, therefore, this is just a factorization, prime factorization of n .

And then the Jacobi symbol $\left(\frac{a}{n}\right)$ is defined as follows; it is defined as like the product from i equal to 1 to k , because they are k prime factors and you actually

complete the Legendre symbol of a with respect to each prime factor and you raise that to the power of corresponding e_i . So, if this is for example, if the i th term of this is p_i to the power of e_i , the i th term of the Jacobi symbol is Legendre symbol of a comma p_i raised to the power of e_i , you understand the definition **right**.

(Refer Slide Time: 06:01)

Example

- Compute $\left(\frac{6278}{9975}\right)$
- Note $9975=3 \times 5^2 \times 7 \times 19$

$$\begin{aligned} \left(\frac{6278}{9975}\right) &= \left(\frac{6278}{3}\right) \left(\frac{6278}{5}\right)^2 \left(\frac{6278}{7}\right) \left(\frac{6278}{19}\right) \\ &= \left(\frac{2}{3}\right) \left(\frac{3}{5}\right)^2 \left(\frac{6}{7}\right) \left(\frac{8}{19}\right) \\ &= (-1)(-1)^2(-1)(-1) = -1 \end{aligned}$$

NPTEL

So, with an example ... So, therefore, for example, if you want to compute 6278 and 9975. So, you are interested in computing the Jacobi symbol then, what I will do is that first of all, I will factor 9975. So, therefore, the prime factorization of 9975 is as follows 3 into 5 square into 7 into 19 **ok**.

So, therefore, from the previous definition this Jacobi symbol is nothing but, 6278 Legendre symbol with respect to 3 and raise to the power of 1 because 3 has a power of 1 here. Similarly 5 is a power of 2, so you compute the Legendre symbol of 6278 and 5 raised to the power of 2 and similarly 6278 Legendre symbol 7, Legendre symbol of 6278 and 19 **ok**.

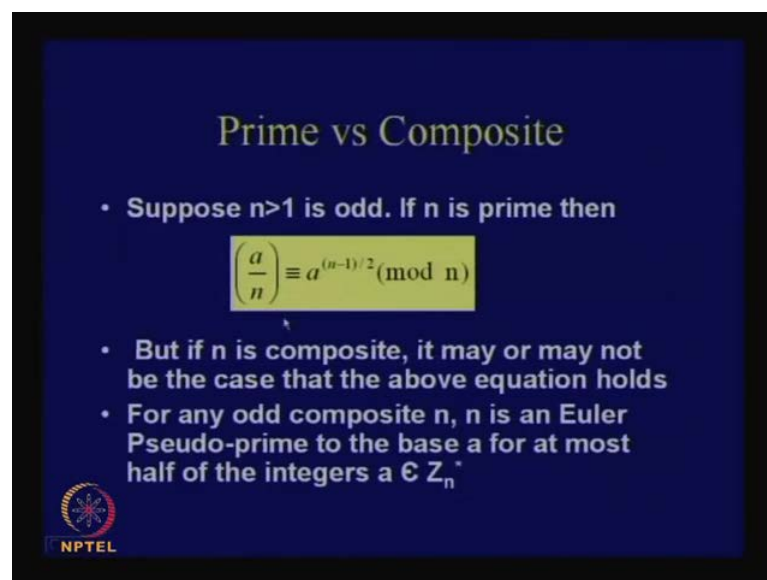
So, now you see that this is actually equal to 2 and 3 is Legendre symbol why because what is this? This is a to the power of p minus 1 by 2, right by my definition and modulo p ; that means, I can do that with a mod p and raised to the power of p minus 1 by 2 also **right**. So, therefore, 6278 if I take a modulo 3 I am and my remainder is 2, I can simplify this stuff. So, therefore, 6278 if I take a modulo with 5, 3 is the remainder **right**. So,

therefore, 6278 similarly if you take modulo 7 with 6 and 6278 if you take modulo 19 is 88.

So, therefore, now this is quite simple to calculate, you will find that all of these values actually are computing to minus 1, why? We can either compute this or check that this is not actually a quadratic residue with this modulo. So, therefore, it is either a non-quadratic residue or you can compute a power p minus 1 by 2, where a is 2 and p is 3. So, all of this compute to minus 1 and therefore, if you will compute this, it will compute to minus 1. So, this is the way how you can compute the Jacobi symbol of 6278 with respect to 9975.

So, you note one thing that in order to compute this Jacobi, what we have done is that actually we have factored out 9975 **right**. So, you appreciate the fact that actually if this number is quite large, certain approach would not work because factorizations I do not know what are the prime factorizations **right** or other its quite difficult for me to compute those prime factors **right**. So, therefore, I need some other way out **right**. So, you understand the problem **right**. So, therefore, but this is how this follows from straight from the definition and this quite **with small (())** with small values.

(Refer Slide Time: 08:37)



Prime vs Composite

- Suppose $n > 1$ is odd. If n is prime then
$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$$
- But if n is composite, it may or may not be the case that the above equation holds
- For any odd composite n , n is an Euler Pseudo-prime to the base a for at most half of the integers $a \in \mathbb{Z}_n^*$

NPTEL

So, now the main fight like prime versus composite how can I differentiate the number from prime, I mean how can I differentiate whether or rather understand whether a

number is prime or composite. So, we give you a result which says like this, that suppose n is greater than 1 n is odd; obviously, if it is even you can straightaway understand it is not a prime number right.

So, if n is prime then I use this result that a n that is the I mean, so, therefore, if n is prime means what. So, if n is prime then what is this Jacobi or Legendre symbols both are same actually, right.

So, therefore, I mean if n is prime then what we can say is that, the Legendre symbol of a with respect to n or the Jacobi symbol that is ok. So, this is actually congruent to a power n minus 1 by 2 modulo n right. So, this is quite ok, I mean this follows straight from the definition of prime numbers right.

But if n is composite, then this actually may be the case or may not be the case because there are some primes which are called pseudo primes which also satisfy this equation. So, therefore, if I use these criteria as a primality testing mechanism, I have to ensure how many such cases are given upper bound of how many composite numbers actually will actually satisfy this equation right.

So, therefore, but if n is composite, it may or may not be the case that the above equation holds for any odd composite n , where n is an I mean if n is an Euler pseudo prime to the base a . So, I call that Euler pseudo prime to the base a for at most half of the integers of a belonging to Z_n^* ok.

So, this is the result. So, therefore, the result says that if we just choose any odd composite number n , then at most there can be half of the integers of a belonging to Z_n^* which will satisfy these things, so not more than half. So, we may wonder why, but these are fact first of all ok.

So, therefore, you understand, first of all understand why how this works that is or why do we need this? Therefore, what we do is that our traveling is that given a random number a which I choose from say Z_n , I am interested to decide that whether that number a is a prime number or not. So, what I do is that I compute the Jacobi of a with respect to n ok.

And then also compute a power $n-1$ by 2 and check whether they are same; if they are same, then I conclude that n is a prime number **right**, but the thing is that as I told you that there are some composite numbers for which also this equality holds or this congruence holds. So, therefore, we need to find out rather I mean, how many such cases or what is the maximum number of such odd composite numbers which will also satisfy this equation **ok**.

So, therefore, this particular last point says is that for any odd composite n , where n is an Euler pseudo prime therefore, it is actually not a prime number it is a pseudo prime. So, it is basically a composite number you can see from this statement itself. So, if you compute the Euler when if you I mean for n is an Euler pseudo prime to the base a for at most half of the integers a , which belongs to Z_n^* . So, let us try to reason out why this is so, ok.

(Refer Slide Time: 12:09)

Error Probability of the algorithm


$$G(n) = \left\{ a : a \in Z_n^*, \left(\frac{a}{n} \right) \equiv a^{(n-1)/2} \pmod{n} \right\}$$

First we shall prove that $G(n)$ is a sub-group of Z_n^* . Hence, by Lagrange's Theorem, if $G(n) \neq Z_n^*$, then $|G(n)| \leq \frac{|Z_n^*|}{2} \leq \frac{n-1}{2}$

Suppose that $a, b \in G(n)$.

$$\therefore \left(\frac{a}{n} \right) \equiv a^{(n-1)/2} \pmod{n}$$

$$\left(\frac{b}{n} \right) \equiv b^{(n-1)/2} \pmod{n}$$

 NPTEL

This is actually an exercise from Stinson. So, I was giving you the solution for that, but this is actually left to as an exercise there, I think there are some more parts, but some parts I have solved here. See for example, you can define like this, that is you can define a set G_n , where G_n is defined like this, that is you take a from Z_n^* and you compute the Jacobi symbol of a with respect to n and actually the congruence satisfies a power $n-1$ by 2 modulo n . So, what does it mean that all these numbers essentially if you choose a and if you apply the previous test will pass **right**.

So, now the question is that whether this G_n is actually I mean is actually I mean all of them are prime or not or what is the maximum cardinality of this particular set, right. So, therefore, first we will prove there actually G_n is the subgroup of Z_n^* . So, if this is so, that is if G_n is actually a subgroup of Z_n^* ; so subgroup means what, subgroup means that it itself a group, if you recall it is itself a group and at the same time it is also closed.

It is a multiplicative group, so and at the same time it is also closed. So, therefore, you see that since G_n is chosen from Z_n^* that is a belongs to Z_n^* . So, it is automatic that it is all the elements are chosen from multiplicity group. So, what do we need to show is there is also closed under multiplication correct.

So, now by if this is so and if we also show that G_n is actually not Z_n^* which means that it is actually small, then I can follow this from Lagrange's theorem, which I stated in the last day's class that actually the cardinality of G_n will be smaller than Z_n^* by cardinality of Z_n^* by 2. Why? What was the statement of Lagrange's theorem? It says that if there is a subgroup then the order of the subgroup divides the order of the group right.

So, therefore, the order of the subgroup is what G_n cardinality and therefore, that has to divide Z_n^* right. So, therefore, the cardinality of this obviously, lesser than the half right you understand that. So, therefore, this cardinality has to be upper bounded by the cardinality of Z_n^* by 2 and cardinality of Z_n^* is maximum equal to $n - 1$ if n is prime it will be $n - 1$. So, I can actually write these inequalities ok.

So, therefore, what we have to show is that G_n is individual subgroup of Z_n^* right and also we have to show that G_n is not equal to Z_n^* , so that means, there is at least 1 element n will belongs to Z_n^* , but which does not belong to Z . Did you understand the idea of the proof?

So, what you have to show is that G_n is individual subgroup of Z_n^* . So, therefore, what we have to show is that the closure property and under multiplication operation and at the same time, you have to show that there is at least 1 element which belongs to Z_n^* , which does not belong to G_n in order to show this inequality.

So, the closure property is quite straight forward **if you** I mean, if you see this property like if you take a and b which belongs to G_n . So, I can write like a Jacobi n will be congruent to a to the power of n minus 1 by 2 mod n , similarly b Jacobi n will be congruent to b power n minus 1 by 2 mod n .

So, now what is the corresponding Jacobi of a into b with respect to n . So, that is actually I mean a multiplicative rule of Jacobi and it is also quite straight forward to understand **why**.

(Refer Slide Time: 15:58)

Error Probability of the algorithm


It follows from the multiplicative rule of Jacobi symbols,

$$\left(\frac{ab}{n}\right) \equiv \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \equiv a^{(n-1)/2} b^{(n-1)/2} \pmod{n} \equiv (ab)^{(n-1)/2} \pmod{n}.$$

$\therefore ab \in G(n)$.

Since $G(n)$ is a subset of a multiplicative finite group and is also closed under multiplication, then it must be a subgroup.

We next show that there exists at least an element in Z_n^* which does not belong to $G(n)$.

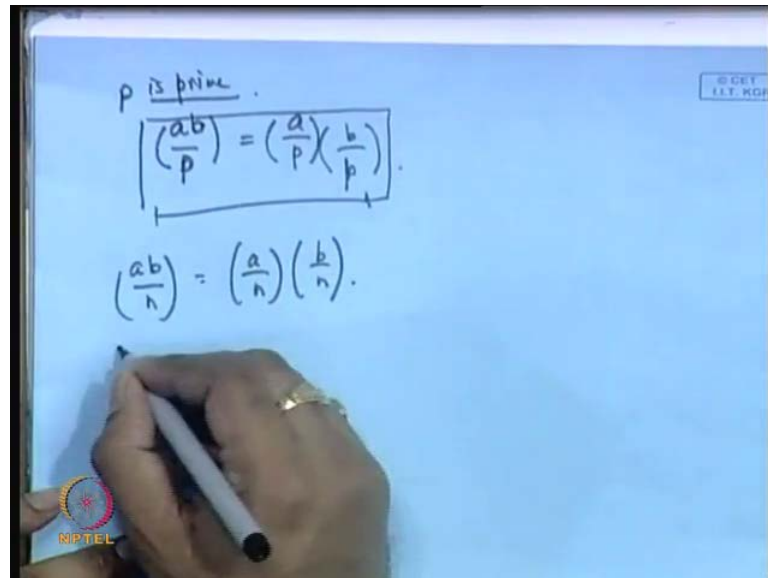
 NPTEL

So, if we apply this, you can actually product I will apply like this, like so you can write like it is a product of a_n and b_n and therefore, this is equal to a power, if this is 2 actually then it is congruent to a power, n minus 1 by 2 into b power n minus 1 by 2 modulo n . And therefore, you see it is equal to $a b$ to the power of n minus 1 by 2 modulo n . So, therefore, $a b$ also belongs to the say group G_n **right**.

So, why does it is to hold? You can understand from the definition of the Jacobi symbol why because the Jacobi was computed by factors of n if you remember **right**. So, therefore, the same factors hold for this and this also **right**. So, therefore, you can actually factor them out term by term and you can split this out like this. So, therefore, and also I mean, what you need to prove is that this result also holds when a, b , when the

Legendre symbol of a b with respect to a prime can be actually factored out in this way, do you follow what I am saying.

(Refer Slide Time: 17:07)



The image shows a hand writing on a whiteboard. At the top, it says "p is prime". Below that, the equation $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ is written and enclosed in a large square box. Below the box, the equation $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ is written. A hand holding a white marker is visible at the bottom left, pointing towards the equations. There is a small logo in the bottom left corner that says "NPTEL".

So, therefore, what I am trying to show is this; that is if that is a prime number p, so p is suppose prime and then, I compute the corresponding Legendre symbol of a b with respect to p, then actually I should be able split this like this, that is a with respect to p and b with respect to p. So, if this result holds, **then also I can** then I can easily write that a b with respect to n is equal to a with respect to n and b with respect to n why? Because I can factor out n, I can factor n and similarly, I can apply the definition of Jacobi symbol, it follows straight from the definition actually.

So, and why this works **this works why this works** is quite easy, because you can straight away apply the other definition of Legendre symbol, which is the I mean a b raise to the power of p minus 1 by 2 and from there it follow straight away. So, therefore, between easy proof of this multiplicative rule for this Jacobi symbol (Refer Slide Time: 18:15).

So, therefore coming back to this proof, so you see that because of this multiplicative property, actually G_n is also closed under multiplication. So, since G_n is a subset of a multiplicative finite group and it is also closed under multiplication, then it must be a subgroup also.

So, what we have next to show is that, there exist at least 1 element in Z_n^* which does not belong to G and therefore you will find that there is an exercise given in your Stinson's book and we have just given you the sketch for that, he says that the question I is like this.

(Refer Slide Time: 18:39)

Error Probability of the algorithm


It follows from the multiplicative rule of Jacobi symbols,

$$\left(\frac{ab}{n}\right) \equiv \left(\frac{a}{n}\right) \left(\frac{b}{n}\right) \equiv a^{(n-1)/2} b^{(n-1)/2} \pmod{n} \equiv (ab)^{(n-1)/2} \pmod{n}.$$

$\therefore ab \in G(n)$.

Since $G(n)$ is a subset of a multiplicative finite group and is also closed under multiplication, then it must be a subgroup.

We next show that there exists at least an element in Z_n^* which does not belong to $G(n)$.

 NPTEL

Suppose n equal to p power k into q , where p and q are two odd prime numbers. So, you see that here it says that p is p and q are odd and p is prime and is also says that \gcd of p comma q is equal to 1, so that means, that p and q do not share any common factor which is a non-trivial factor. So, therefore, now if you define a which is equal to 1 plus p to the power of k minus 1 into q , then you can easily see that a belongs to Z_n^* , why? Because if you take a and if you take the and if you observe n , then this n and this particular a cannot share any common factor common non-trivial factor. So, a belongs to Z_n^* **ok.**

So, what we now **next to** next need to show is that a does not belong to G_n , so that means, what we have to show that if I take a and if I compute the Jacobi of a with respect to n this should not be congruent to a power n minus by 2 modulo n **right.**

Yes. So, therefore, what we do is that you take a and take n and you need to compute the Jacobi symbol. So, you know the factors of n right, it is p power k into q . So, therefore, you can apply this straight away and you see that this is actually equal to 1 because a

with respect to p is 1 and a with respect to q is 1, why? Because if you take modulo p and modulo q only 1 remains **right**. So, therefore, this is equal to 1.


So, therefore, the right hand side that is a power; so therefore, this is actually, what is the right hand side of what we are checking? It is a power $n - 1$ by 2, so this we can actually do from binomial theorem **right**. Because a is what $1 + p$ to the power of $k - 1$ into q . So, if I need to compute a power $n - 1$ by 2, I can apply to the power of $n - 1$ by 2 and do a binomial expansion of this **3 right**.

So, therefore, you will see that this binomial expansion if you take a modulo n , then only these 2 terms remain, the other terms vanish why? Because k is actually greater than equal to 2 by my definition, all the higher terms will be actually if you take modulo n will be divisible by and will become the remainder will be 0. So, you can check this actually **um**.

So, therefore, the only 2 terms which will remain is $1 + n - 1$ by 2 into p to the power of $k - 1$ into q modulo n . So, now, if this and this has to be equal that is if a Jacobi n has to be equal to a power $n - 1$ by 2, then the second term has to go to 0 **right**. So, therefore, n has to divide this number **right**.

So, n what is n ? n is p to the power of k into q . So, therefore, p to the power of k into q has to divide $n - 1$ by 2 into p to the power of $k - 1$ into q **right** and therefore, p has to actually divide $n - 1$ by 2 **ok**.

(Refer Slide Time: 21:47)



Error Probability of the algorithm

Suppose, $n = p^k q$, where p and q are odd, p is prime, $k \geq 2$, $\gcd(p, q) = 1$. Let, $a = 1 + p^{k-1}q$.

We have, $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)^k \left(\frac{a}{q}\right) = 1$.

Using Binomial theorem,

$$a^{(n-1)/2} = \sum_{i=0}^{(n-1)/2} \binom{(n-1)/2}{i} (p^{k-1}q)^i \equiv 1 + \frac{n-1}{2} p^{k-1}q \pmod{n}$$

[as $k \geq 2$, the other terms in the Binomial expansion are $0 \pmod{n}$]

And therefore, you can rearrange this and find out the n as in that case congruent to 1 modulo p , how? Because n minus 1 by 2 has to be some integer multiple with p , right so its $k p$ something. So, therefore, n is equal to 1 plus 2 $k p$. So, if you take a modulo of p on both sides, then n is actually equal to congruent to 1 mod p .

But we know that n is actually 0 mod p because n was what p to the power of k into q . So, we have a contradiction and were therefore, this equality is not correct. So, therefore, a does not belong to G_n right and what does it mean? It means the G_n and Z_n^* are not the same, **right**. And therefore, we can apply the Lagrange's theorem and from there we can say that the cardinality of G_n is actually lesser than equal to n minus 1 by 2.

So, now this is the main idea. So, therefore, you see that idea is that, I mean less than half of the numbers can be at most there can be n minus 1 by 2 numbers which will satisfy this test. So, therefore, I can apply this test with a **with a with a** good probability of success.

(Refer Slide Time: 23:17)


Error Probability of the algorithm

$$\text{If, } \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$$
$$\Rightarrow \frac{n-1}{2} p^{e-1} q \equiv 0 \pmod{n}$$
$$\Rightarrow p^e q \mid \frac{n-1}{2} p^{e-1} q \Rightarrow p \mid \frac{n-1}{2} \Rightarrow n \equiv 1 \pmod{p}.$$

But this contradicts the fact that $n \equiv 0 \pmod{p}$.

Thus although $a \in \mathbb{Z}_n^*$, it does not belong to $G(n)$.

Thus, $|G(n)| \leq \frac{n-1}{2}$.



So, therefore, you will see how this algorithm works in more details, I just given you this **I mean...** So, therefore, let us go through this therefore, it says suppose n is a composite number therefore, there can be 2 cases: a belongs to \mathbb{Z}_n difference \mathbb{Z}_n^* . That means, a belongs to \mathbb{Z}_n difference \mathbb{Z}_n^* means what a is not co-prime to n right. So, in that case, gcd of a comma n is what not equal to 1 and therefore, a Jacobi n will be 0.

Why? Because in that case it means that, if I factor out n , there should be 1 factor for which this will be 0, right; if you factor n into its prime factors, then one of the terms 1 of the product terms has to go to 0. So, therefore, from there it follows. Therefore, it shows that there is a non trivial division. So, therefore, you know that this number a is actually not a rather is a composite number. So, therefore, you understand easily this is a correct answer, this is a composite number.

Now, what about the next case when a belongs to \mathbb{Z}_n^* then gcd of a comma n is actually not equal to 1 **right sorry** gcd of a comma n is equal to 1. So, in that case solovay strassen can return a wrong answer if and only if a belongs to G_n **right**. So, what we have proved is that, cardinality of G_n is maximum equal to n minus 1 by 2 and from there I can compute the probability of a wrong answer to be maximum equal to half that is the rational behind a solovay strassen algorithm **ok**.

(Refer Slide Time: 25:18)

Error Probability of the algorithm

Suppose, n is composite. If, $a \in \mathbb{Z}_n^* \setminus Z_n^*$,
 $\text{gcd}(a,n) \neq 1 \Rightarrow \left(\frac{a}{n}\right) \equiv 0$, thus algorithm gives always
correct answer.

If, $a \in Z_n^*$, thus $\text{gcd}(a,n) = 1$, Solovay Strassen returns wrong
answer if and only if $a \in G(n)$. We proved that $|G(n)| \leq (n-1)/2$.
Thus, the probability of a wrong answer is:

$$\frac{|Z_n^* \setminus G(n)|}{n-1} \leq \frac{1}{2}$$

NPTEL

So, now if you understand this, I mean the rest of the thing will be quite easy to follow. So, this is an example of a pseudo prime number for example, if you take 91 and if i take to show you that really such kind of numbers exist. So, gcd of 10 comma 91 is actually equal to 1. So, therefore, if this would have been something like a I mean, since this is equal to 1, we apply our check.

So, therefore, it says that 10 and 91, if I compute the Jacobi it comes out to minus 1 and if you do 10 to the power of 91 minus 1 by 2 and take a modulo 91, this also comes out to minus 1. So, therefore, this satisfies my check, the solovay strassen check, but you know that 91 is actually not a prime number, right there are non-trivial factors. So, if gcd of a comma n is greater than 1 then a and n have at least 1 common prime factor.

So, therefore, this is actually quite easy to understand why it is so, and we have understood why and that is the Jacobi of a to the base of n is 0 and the condition is actually if and only if so, therefore, this condition is actually if and only if. So, thus if Jacobi is 0 with respect to any a then n is composite, but remember the choice of a is random. So, this is what I told you that if the Jacobi computes to 0 then that means, there is a particular factor in the prime factorization of - if a factor n into say prime factors and therefore, in the computation of the Jacobi symbol there is 1 factor which goes to 0 **right**.


(Refer Slide Time: 26:17)

Example

- 91 is a pseudo prime number to the base 10
- Note that $\gcd(10,91)=1$

$$\left(\frac{10}{91}\right) \equiv 10^{(91-1)/2} \pmod{91} \equiv 10^{45} \pmod{91} \\ \equiv -1$$

- If $\gcd(a,n)>1$ then a and n have at least one common prime factor. Thus the Jacobi of a to the base n is 0. The condition is actually if and only if. Thus if Jacobi is 0 with respect to any a , n is composite. But remember the choice of a is random.

 NPTEL

So, therefore, this follows from this fact that, if I take n and if I compute like p_1 to the power of e_1 , p_2 to the power of e_2 and so on till t k to the power of e_k and I am interested in computing the a Jacobi n , then what does it mean? I am computing I equal to 1 to k , a with respect to p_i and raised to the power of e_i .

So, now if this computes to 0 it means that there exist a p_i or other there exist i for which $a \cdot p_i$ is equal to $0 \pmod{p}$ right and what does it follow from the definition? Definition is what? The definition is it implies the a is congruent to $0 \pmod{p}$ **right** this follows from the definition, you remember the definition of Legendre symbol; it says that a within that symbol p is congruent to 0 if a is congruent to 0 modulo p rest of the cases it is plus 1 or minus 1. That means, easily that there is a non-trivial factor of a . So, therefore, what is a ? Can be a prime number, a is definitely a composite number **ok**.

(Refer Slide Time: 27:35)

The slide is titled "Example" and contains the following text:

- 91 is a pseudo prime number to the base 10
- Note that $\gcd(10,91)=1$

$$\left(\frac{10}{91}\right) \equiv 10^{(91-1)/2} \pmod{91} \equiv 10^{45} \pmod{91}$$
$$\equiv -1$$

- If $\gcd(a,n)>1$ then a and n have at least one common prime factor. Thus the Jacobi of a to the base n is 0. The condition is actually if and only if. Thus if Jacobi is 0 with respect to any a , n is composite. But remember the choice of a is random.

NPTEL logo is visible in the bottom left corner.

So, therefore, this check is quite easy, this is always correct in terms of composite decision problem that whether a number is composite or not, this is always a correct answer **right**. **So, if this is not** so, that if it is not equal to 0, then there is a chance of making an error because we apply the next check and you know that because pseudo prime numbers exist what you return is actually may be wrong **right**.

But, if you say that a number is actually composite, then it is true because if I find out that for a given number a Jacobi n is not congruent to a power n minus 1 by 2 modulo n then definitely a is a composite number **right**, but the problem is other way round; if it is satisfy then to understand whether a number is prime or a number is composite, then there is a chance of making a mistake. And what we have showed just now is at the probabilities of making an error is maximum half that is the reasoning of the solovay strassen algorithm **ok**.

So, you see that if this number if this algorithm says to you that a given number is a composite number, it is always correct. So, therefore, this is an example of a.

(())

(Refer Slide Time: 29:24)

p is prime.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

$$\left(\frac{a}{n}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{e_i} = 0$$

$$\exists i \text{ s.t. } \left(\frac{a}{p_i}\right) \equiv 0 \pmod{p_i}$$

$$\Rightarrow a \equiv 0 \pmod{p_i}$$

It is based on monte-carlo algorithm. So, this is the summary of whatever I told you just now, that however, if a Jacobi is not 0, then we check whether it is actually equal to a power $n - 1$ by 2 modulo n ; if no then it is definitely composite, but if yes it can be prime, it can be pseudo prime **ok**.

So, it can be pseudo prime in that case, what we are doing is that we are saying it is prime. So, the result can be erroneous and that is an error probability, but if we say that whenever it saying yes, it is actually correct. So, this problem is with respect to I mean not is prime, but whether is composite that where a number is composite or not.

So, luckily we have the following fact that if the Jacobi symbol is not 0 with respect to a then $\gcd(a, n)$ is actually equal to 1. So, therefore, if a Jacobi is not 0 with respect to a , then the $\gcd(a, n)$ is equal to 1. So, this we have already told you and so a belongs to \mathbb{Z}_n^* and for any odd composite n , n is an Euler pseudo prime to the base a , for at most half of the integers a belonging to \mathbb{Z}_n^* . Thus we have the following monte-carlo algorithm with error probability of at most half. So, this is what I am trying to argue till now actually.

(Refer Slide Time: 30:41)

Legendre Symbol

Suppose p is an odd prime. For any integer a , define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Suppose p is an odd prime. Then

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

NPTEL

So, this is the working of the algorithm, it says it is a solovay strassen algorithm. So, you see that if choose the random integer a , such that $1 \leq a \leq n-1$. So, for the first step what you do is that, you compute the Jacobi of a with respect to n if this is actually equal to 0, then immediately you can say that n is composite.

(Refer Slide Time: 32:33)

Legendre Symbol

Suppose p is an odd prime. For any integer a , define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Suppose p is an odd prime. Then

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

NPTEL

Do you understand this? So, therefore, what is the other case, you take y and you compute $a^{(p-1)/2} \equiv y \pmod{p}$ rather mod n , then you can

return that n is a prime number, otherwise you say that n is a composite number. So, you see that whenever it says a composite number like this case or this case, it is a correct answer, but if it says n is prime then, there is a chance of making a mistake. So, the decision problem is n composite. So, that is the composite problem. So, note that whenever the algorithm says yes, the answer is correct. So, error may occur, when the answer is no and the error probability is at most half, you understand this.

So, now you see that, we need to compute this Jacobi symbol right so, but what we have seen is that computing the Jacobi symbol requires the factorization of n , but we know that factoring n is a hard problem itself **right**.

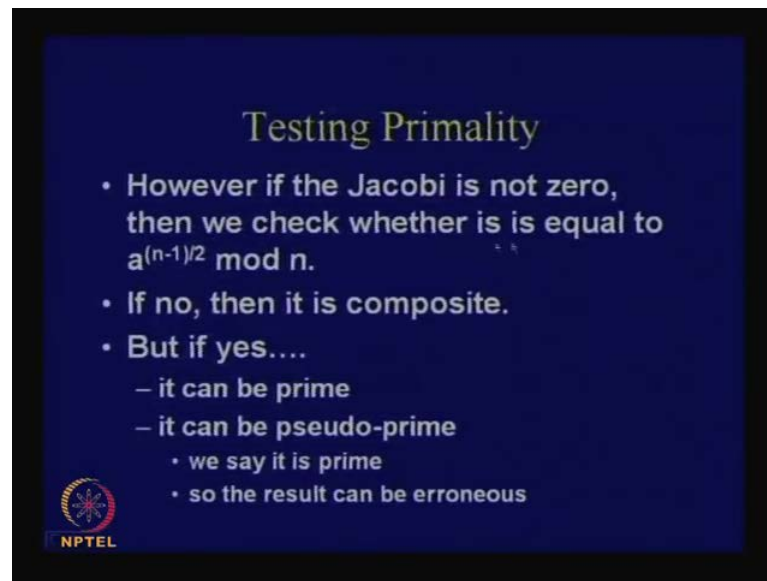
But luckily from number theory, we have actually some properties through which we can always compute the Jacobi symbol. So, I am not going into the proofs of this properties, but it follow straight away from the I mean in order to prove this for the Jacobi symbols, you have to prove it for the Legendre symbols. And the proof for the Legendre symbol is quite straight forward; you can work it out and take it as an exercise **ok**.

So, this I have already told you why, I mean this multiplicative property which we have applied for the previous thing and this also is quite straight forward to follow **right**. So, we can just go through them step by step, it says that if n is a positive odd integer and m_1 is congruent to $m_2 \pmod{n}$, then if you need to compute m_1 Jacobi n , then what you do is that you take modulo n and you compute m_2 modulo n **ok**.

So, therefore, suppose that m_1 is greater than n , you can do this **right**. So, therefore, you can take a modulo n and bring it inside n , bring it inside \mathbb{Z}_n and then you compute m_2 with respect- I mean Jacobi of m_2 with respect to n and there is another interesting result which says that 2 n 's Jacobi if n is congruent to 1 . So, you see that n is a positive odd integer. So, if n is a positive odd integer, so you see that for all of this cases, n is the positive odd integer because that is the only case if it is even number, then there is no problem **right**.


So, if n is a positive odd integer then the Jacobi of 2 with respect to n is actually either plus 1 or minus 1 and there can be total two cases, where n is equal to plus minus $1 \pmod{8}$ or n equal to plus minus $3 \pmod{8}$ **why** can there will be only 2 cases? So, I told you that n is a odd number **right**. So, there are four possible factors you see that.

(Refer Slide Time: 34:14)



Testing Primality

- However if the Jacobi is not zero, then we check whether it is equal to $a^{(n-1)/2} \pmod n$.
- If no, then it is composite.
- But if yes....
 - it can be prime
 - it can be pseudo-prime
 - we say it is prime
 - so the result can be erroneous

 NPTEL

So, what I am saying is that if you take mod 8 right, then what are the possible remainders, it is 0 1 2 3 4 5 6 and 7. So, this I can also write as 0 1 2 3, this is I can write as 4, this is I can write as minus 3, this is what minus 2 and this is minus 1. So, what are odd numbers here? In this case the odd numbers are this, **this** and this (Refer Slide Time: 34:38). So, what are the corresponding remainders? It is 1, it is 3, it is minus 3 and minus 1. So, you have got 1, 3, minus 3 and minus 1 as the possible remainders.

So, therefore, there are 2 cases here; n is congruent to plus minus 1 mod 8 and n equal to congruent to plus minus 3 mod 8. So, in these 2 cases, this continues to either plus 1 or minus one.

Similarly, if n is a positive odd integer then you can apply actually like this, but what is more interesting to note is that, if you can write n like this like $2^k \cdot t$. So, you see that in this case, what I am computing is that n and Jacobi of m with respect to n and suppose I can, so if n is a even number then, I can factor out all the 2 powers that is all the factors of 2 and remain and I mean and so if I factor out all the possible 2 factors, then I will be remained with - what will be remaining - an odd factor right.

So, therefore, t is that odd factor and therefore, you can express n as $2^k \cdot t$ and therefore, m Jacobi of m with respect to n will be 2 Jacobi of 2 with respect to n multiplied I mean whether raised to the power of k , multiplied with t with I mean Jacobi

of t with respect to n . So, this follows straight away from the multiplicity proof and why it works is quite simple.

So, what about this, that is if m and n are positive odd integers, then if you are interested in computing the Jacobi of m with respect to n , then it is either minus Jacobi of n with respect to m or plus Jacobi of n with respect to n and there can be 2 cases that is n is congruent to n congruent to $3 \pmod{4}$ or otherwise. So, you can again follow similarly why there can be only 2 cases. So, therefore, it is either equal to minus - so, you see that what you are doing is that you are computing the Jacobi of n with respect to m with a - plus sign or minus sign as be the case, ok.

So, can you now say that how can I use this to compute a Jacobi of any 2 integers. So, you see that what will I first do? First if m is greater than n , then I will apply this result and bring it within n ; I am not talking about the trivial cases. There are some trivial cases, which can straight away said 0 or 1, leaving those cases, I am talking about non trivial cases, you take a modulo n apply this do it ok.

Next thing is that you check this, whether this number is an even number or not; if this is an even number, then you apply this result and factor out all the 2 powers and you are remaining with an odd integer value and so you compute recursively the Jacobi of this and this right. So, now, you are actually **you have got** you have to solve this sub problems right. So, in order to solve this sub problem you apply property 4, ok.

(Refer Slide Time: 37:50)

Solovay-Strassen Algorithm

```
SOLOVAY-STRASSEN(n)
choose a random integer a such that  $1 \leq a \leq n - 1$ 
 $x \leftarrow \left(\frac{a}{n}\right)$ 
if  $x = 0$ 
  then return ("n is composite")
 $y \leftarrow a^{(n-1)/2} \pmod{n}$ 
if  $x \equiv y \pmod{n}$ 
  then return ("n is prime")
else return ("n is composite")
```

The decision problem is "Is *n* composite?".
Note that whenever the algorithm says "yes", the answer is correct.
Error may occur when the answer is "no" and the error probability is at most 1/2.

NPTEL

So, this is an example to show you how it works. Suppose, I am interested in computing 7411 and Jacobi of that with respect to 9283; so, here you see that 7411 is actually smaller than 9283. So, therefore, I have applied property 4 and I do a minus of this. So, why minus, because of the check that is in this case, minus was if *m* and *n* both are congruent to 3 mod 4 ok.

So, if you divide both of them by 4, you will get a remainder of 3. So, believe me for this right now. So, therefore, it will be minus this and this (Refer Slide Time: 38:25). So, therefore, now you see that this number is greater than 7411. So, what we do? We take a modulo of this number with 7411 and we are remaining with this particular remainder. So now, you need to compute this Jacobi.

So, you see that this number is actually even number. So, what I can do is that, I can factor out all the 2 powers and this is what all I am remind with; therefore, I have a two smaller problems to solve now. So, therefore, now this number I mean this is actually you can easily follow what is the corresponding result for this, why?

Power slope

Yeah, you can apply straight away this result and therefore, you can apply basically property three; I mean so, therefore, this follows directly from property 2 actually ok.

So, therefore, what do I mean, so property 2 is this that is in order to compute 2 with respect to Jacobi n , what you have to done is that it is either plus 1 or minus 1. So, there can be only two cases when you are computing the Jacobi of any odd positive integer with respect to 2. So, therefore, in this case it is if it is equal to so if you take a modulo 8. So, therefore, if you take a modulo 8 means, you take 741 modulo 8, what is the remainder? 3 so, therefore, it follows in this particular class, it is actually equal to minus 1.

So, it does not matter actually because we have raised to it power 4. So, it is either minus 1 power 4 or plus 1 power 4 you we will definitely get 1. So, therefore, now you have to solve this problem that is Jacobi of minus 117 with respect to 7411. So, now, what will you apply? You apply the 4th property and then again apply bring it like this. So, you know you say this is actually greater than this **right**.

So, what you do is that you take a modulo of 7411 with respect to 117 and this becomes 40 with respect to 117 and similarly you can again observe that 40 is a even number. So, you can factor out like 2 power 3 into 5 and therefore, you can apply this result like you can. So, therefore, again the previous computation or the rather property 2 can be applied and you can compute that this will be 5 Jacobi with respect to 117 and similarly the rest of the things follows. So, therefore, you will find that minus 1 will be the final result **ok**.

So, what the idea is that you can actually compute the Jacobi of any of any 2 integers without actually factoring out in, that is the idea and does it remind you of any algorithm like the way how you are computing this.

(())

Yeah. So, therefore, this is actually like the Euclidean algorithm itself. So, in the Euclidean algorithm, what was the maximum number of times you did that operation? It was actually log of n , right number of times we are doing that operation because you are dividing like that **right** because every time there is a chance that you are dividing by you are you are basically reducing your problem, **right** the number of steps was in logarithm with respect to the input size.

Similarly, here also you can reason out that the number of steps you are requiring to do this that is you are requiring doing this modulo operation will also be logarithm with respect to n , why? Because in the first case also only if $m-1$ is greater than n you are doing a modulo **right** straight away. So, therefore, your problem size reduces to the field size of \mathbb{Z}_n . So, therefore, your input size is in this case with respect to \mathbb{Z}_n , the size or cardinality of \mathbb{Z}_n and that is n . So, therefore, you will see that the number of times you are actually applying this modulo operation can be at most equal to $\log n$.

So next is a property 4.

Property 4, so property 4 is m by n **right** what you are trying to compute is a Jacobi of m with respect to n and what you are seeing here is that m there can be two cases. So, it says that minus m by n or n by m . So, now, what I am saying is that in order to prove this result, first of all you have to prove that this also holds for the Legendre symbol **ok**.

So, therefore, in that case, assume that n is a prime number and you compute this. So, there are this is actually follows from I mean is a number theoretic result, but you can try that I mean it is not so difficult. I mean, so what you can do is that, you can you need to compute a power or rather m power $n-1$ by 2, where n is a prime number and there you can plug-in these two things like n is congruent to n is congruent to $3 \pmod{4}$; so that means, you have to write this as like say for example, if it is a multiple of 4, then it will be like $4k$ or $4k+1$, $4k+2$ and $4k+3$. So, this if it is equal to 3 it will be $4k+3$, **right**. So, you plug in this values it will come out to this. So, I am leaving the details of the proof to you as an exercise, you can do that.

(Refer Slide Time: 43:35)

Rules to be remembered

1. If n is a positive odd integer and $m_1 \equiv m_2 \pmod{n}$, then
$$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right).$$
2. If n is a positive odd integer, then
$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8} \\ -1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$$
3. 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 $m = 2^\delta t$ and t is odd, then
$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^\delta \left(\frac{t}{n}\right).$$
4. Suppose m and n are positive odd integers. Then
$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{t}{n}\right) & \text{if } m \equiv n \equiv 3 \pmod{4} \\ \left(\frac{t}{n}\right) & \text{otherwise.} \end{cases}$$


NPTEL

So, now I have arranged this, whatever I told you is in form of an algorithm. It says that, if your input n is greater than equal to 0 n is greater than equal to 1 and n is odd I am interested in computing this Jacobi symbol of m with respect to n if n is equal to 0, then these two results are quite straightforward, you can easily withdrawn this results, else if n is greater than n then what it do is that you return the Jacobi symbol of m modulo n with respect to n , else you factor out m in this fashion like m equal to 2 power δ into m dash, where m dash is an odd number greater than equal to 1. Then you written the Jacobi symbol of 2 comma n with power to the δ any raised to the power of δ and Jacobi symbol of n comma m dash **ok**.

So, then you use that either a plus 1 here or a minus 1 here depending upon property 4 **right**. So, therefore, I think I made a mistake here, n dash is congruent n is congruent to 3 modulo 4. So, it is either minus 1 otherwise it is a plus. **So**, So, you see that the main thing is that you are basically computing the Jacobi without factoring n . So, that is the main beauty of this algorithm and why this algorithm has got $o \log p$ step, I think it is clear to you and each modulo operation will have the actually $o \log$. So, there is a division involved **right**.

(Refer Slide Time: 14:17)

An Example

$$\begin{aligned}
 \left(\frac{7411}{9283}\right) &= -\left(\frac{9283}{7411}\right) && \text{by property 4} \\
 \cong &= -\left(\frac{1872}{7411}\right) && \text{by property 1} \\
 &= -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) && \text{by property 3} \\
 &= -\left(\frac{117}{7411}\right) && \text{by property 2} \\
 &= -\left(\frac{7411}{117}\right) && \text{by property 4} \\
 &= -\left(\frac{40}{117}\right) && \text{by property 1} \\
 &= -\left(\frac{2}{117}\right)^3 \left(\frac{5}{117}\right) && \text{by property 3} \\
 &= \left(\frac{5}{117}\right) && \text{by property 2} \\
 &= \left(\frac{117}{5}\right) && \text{by property 4} \\
 &= \left(\frac{2}{5}\right) && \text{by property 1} \\
 &= -1 && \text{by property 2.}
 \end{aligned}$$


So, therefore, the complexity of doing a division will be $O(\log p \text{ whole square})$. So, therefore, or $O(\log n \text{ whole square})$. So, the total complexity of this algorithm will be in that case $O(\log n \text{ whole cube})$. So, this is a very light bound that I am giving you it is not. So, tight calculation, but overall is $O(\log n \text{ whole cube})$. So, this is a polynomial type algorithm **right** to compute the Jacobi symbol. So, roughly its $O(\log n \text{ whole cube})$ and this is these are the details **ok**.

So, now we will conclude with one more application like I mean **so what we**, so, what is my problem? Now we have a tool right that given a or question that whether a number is composite or not. I can apply the solovay stressen algorithm and with a probability of error probability of at most half, I can say whether the number is composite or not **right**.

Now, the question is whether the number is composite or not, if you if I say it is composite is always correct, but sometimes I will say its prime also **right**. So, in that case there is an error probability because it can be correct, it may be wrong also and the error probability is at most half **right**. So, what comes to our mind now? I will repeat this experiment, right and I need and I would like to magnify my correctness right.

So, therefore, now you can in order to compute this, **what we are I** I will define 2 events like this (Refer Slide Time: 46:10). So, a is 1 event and b is another event. So, what is a? a is that event which says that a random odd integer n of specified size is composite. So,

let this a be the event a that is I choose a random odd integer n of a specified size and that is composite **ok**.

Similarly, I choose I mean b is that other is another event which says that the algorithm answers n is prime m times in succession. So, if I am repeating the solovay-strassen test for n times, m times in succession, the algorithm answers that n is a prime number **ok**. So, therefore, probabilities of b given a is actually upper bounded by 2^{-m} because each times it is half right. So, therefore, it is lesser than half for each case and all many of them are independent applications **right**.

So, therefore, this probability of b given a is a conditional probability is lesser than equal to 2^{-m} **right**, but what we are interested is in the probability of a given b. What is a given b? It is that a random odd integer n of specified size is composite given that m times in succession the experiments has told you that it is a prime number **right**.

(Refer Slide Time: 48:40)

Computing Jacobi without factorization of n

- Input: $m \geq 0, n \geq 1, n$ odd
- Output: `JacobiSymbol(m,n)`

```
if(m==0)
  { if(n==1) return 1; else return 0;}
else if (m>n)
  return JacobiSymbol(m mod n, n);
else{ m=2bm'; (where m'≥1, m' odd)
  return ±[JacobiSymbol(2,n)]b[JacobiSymbol(n,m')]
/* Use -, if m'≡3 (mod 4), + otherwise */}
```

NPTEL

So, therefore, what we do for this? We apply the Bayes' theorem. So, you know that for Bayes' theorem I will meet the value of probability of a. So, what is probability of a? The probability of a is the random odd integer n of specified size is actually composite. So, for that we can apply prime number theorem **right**. So, if I apply that then, what we get is that this probability because of the previous discussion and since we have taken only odd

integers it will be $2^{1/n}$. So, therefore, the probability of a is actually almost equal to $1 - 2^{1/n}$ because what we are saying is now that composite right, a is a composite number **right**.

So, a is what? This is a random odd integer n of specified size is composite and what we got from here is that it is a prime number. So, you take $1 - 2^{1/n}$ of that it roughly gives you the probability that an odd integer is composite **ok**. So, now you can straightforward apply the Bayes' theorem, it says product of a given b is equal to probability of b given a into probability of a divided by probability of b. So, now, I am not going into that details, we can see that work out it follows straight away from the base theorem, but the thing is that you have got the reasonably configured equation now formula now **ok**.

So, but the thing is that, what we will do is that, we will plot this with respect to $2^{1/n}$ minus $2^{1/m}$. So, we will plot with respect to $2^{1/n}$ minus m and see which one falls first, you see that this is what is done $2^{1/n}$ minus m and the bound on the error probability.

So, you see that although it really does not decay like $2^{1/n}$ minus m, but it still also decays quite fast and you see that for numbers of these ordered like, if you have do it for 50 times or 100 times, then you are error probability is actually quite small. So, you see that both becomes fairly small and negligible values and can hence be neglected.

So, therefore, if I apply the solovay-strassen algorithm, I will not apply it for 1 or 2 times, but apply it for say 100 times and if 100 applications for m, for each number of times, if the result says you that it is a prime number, I will assume that it is a prime number and this gives me an upper bound of the probability and I remember that there is an error probability in that, but I will take it.

So, you see that we have reasonably good and this is actually quite a primitive algorithm there are much more developments over this. So, therefore, you see that, but these are very nice algorithm in order to understand the basics of primality testing. So, what we have followed as the reference is the Stinson book. So, you can go back and read this and next is we will discuss about some factoring algorithms.