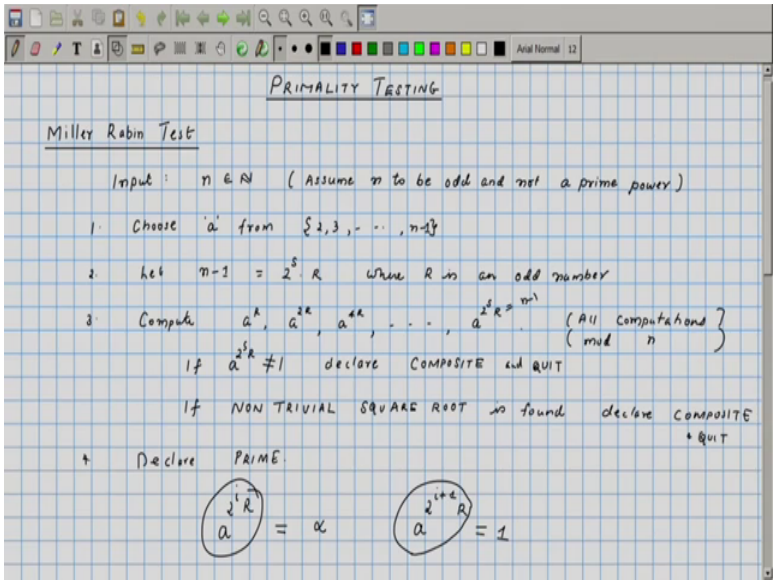
Randomized Algorithms
Prof. Benny George Kenkireth
Department of Computer Science & Engineering
Indian Institute of Technology, Guwahati

Lecture - 25
Miller Rabin Algorithm

We were looking at the Miller Rabin Test in the previous class.

(Refer Slide Time: 00:38)



So, the steps in Miller Rabin are as follows, if the so we will assume that the input as a an odd number and not a prime power. We choose a random a and compute a raised to R, a raised 2R, a raised to 4R and so on, up to a raised to 2 to the S R 2 to the S R is equal to n minus 1.

If all if after all these computations, if we find that a raised to n minus 1 or a raised to 2 to the S times R is not equal to 1, in that case we declared as composite. And in between if in any of the steps we find a non-trivial square root of unity, then also we declare that the number as composite. These are genuine conditions under which we can declare the number as composite, because for any for a prime number a raised to n minus 1 must be equal to 1, and a prime number must not have any non-trivial square root of unity.

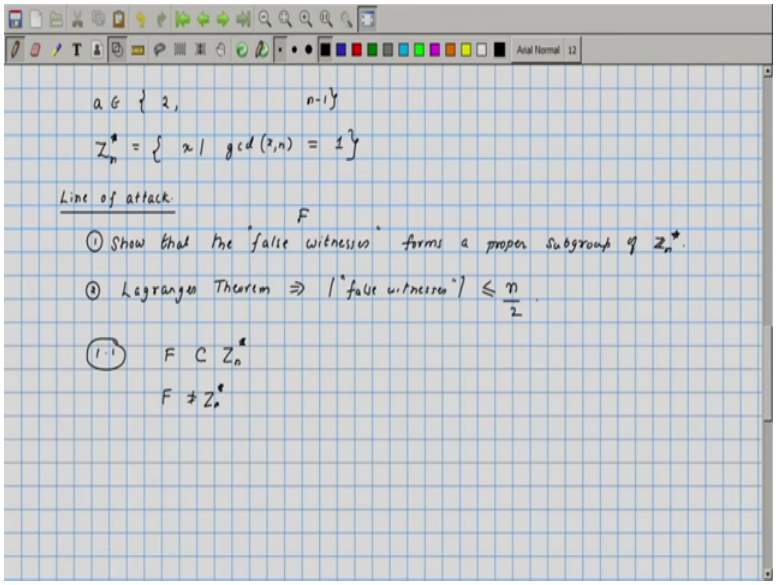
Non-trivial square root of unity means, we found some numbers such that a raised to 2 to the i times R is equal to let us say alpha, where alpha is not equal to plus or minus 1 , but

a raised to 2 to the i times 2 or i plus 1 times R. So, a raised to 2 to the i plus 1 times R is equal to 1, this would mean that alpha is a non-trivial square root of unity.

Now, we have argued in the last class that primes if you take n to be a prime number, then there would not be any non-trivial square root of unity that is there cannot be any numbers other than 1 and p minus 1 with squared gives us identity. Here this number a raised to 2 times i to a raised to 2 to the i times R that turns out to be a number which is not plus 1 or minus 1 or p minus 1, but square it gives us 1 ok. So, these are both genuine conditions under which we will declare the number as composite.

And if these conditions are not met, then we had declared it as prime. What we need to argue is that on every composite number, this algorithm correctly declares it as composite with more than 50 percent chance. It is clear that this algorithm will say the correct answer for every prime number, because a prime number will not be declared composite ever by this algorithm. So, the only error with this algorithm can make is declare a composite number as a prime number. We will show that that happens with less than 50 percent chance ok.

(Refer Slide Time: 03:34)



So, in the algorithm we chose the a from the set 2 to n minus 1 ok. Now, let us look at this question if n was a composite number, then how many of these a's will pass these tests. So, if you call this is test 1 and this is test 2, how many of these a's will pass the test. So, the a's which pass the test essentially bears a false testimony to the primness of

n. So, n was actually not prime, but just because the a that we chose pass this test, we would incorrectly declare the number n as prime.

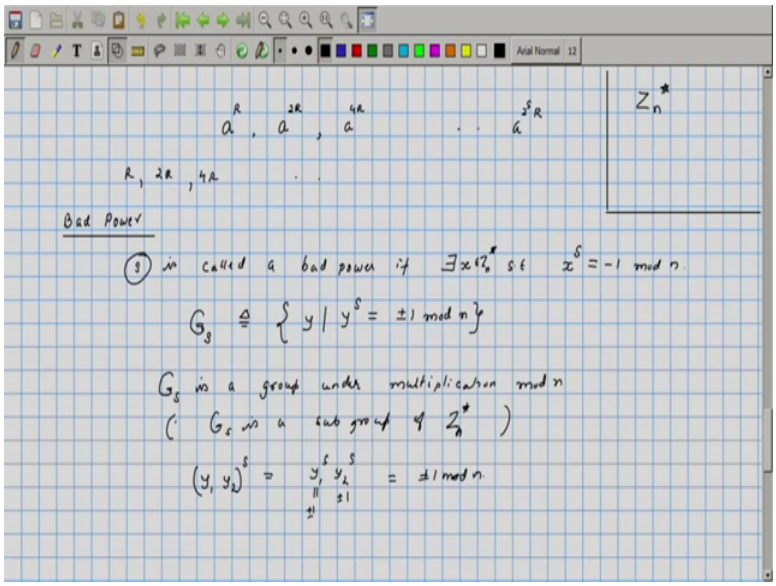
So, we want to count the number of false witnesses and we want to say that they form a very small set, so that would also mean that the other elements which would correctly testify that the numbers are composite, they are large collection. We will show that at least 50 percentage of the numbers, we will correctly identify the number to be composite. In order to show that what we will what we will essentially show is that these numbers which bear false testimony to the primness of n will be a sub group of a certain group, it will be a proper subgroup of a certain group.

So, if you look at the group Z n star ok. So, this is the set of all elements such that gcd x, n is equal to 1 ok; we will assume that x lies between 0 to 1 to n minus 1, so x belongs to the set 1 to n minus 1 ok. So, take all these elements that is your Z n star and what we will show is that the set of false witnesses, this is strict subgroup of Z n star, so that is our line of attack show that the false witnesses forms a proper subgroup of Z n star ok.

So, any proper subgroup its size must divide the size of the group. And therefore, Lagrange so that is Lagrange theorem, so Lagrange theorem says that would imply that size of the set of false witnesses. So, we look at the set of all false witnesses the set of so that is set it size will be less than say n by 2 ok, because Z n size is at most n ok. And the false witnesses since it is a strict subgroup, its number must divide the group the size of the entire group. So, it is going to be less than n by 2 ok.

So, now how do we show that this collection of false witnesses is a proper subgroup. First we will show that it is a subgroup, so we can write this as 2, subgroup 1.1 would be so let me call this as F. So, F will be a subgroup of Z n star and then we will show that F is not equal to Z n star, so that would mean that it is a strict subgroup. So, we will exhibit one element which belongs to Z n star, but it is not belonging to F ok.

(Refer Slide Time: 08:09)



So, let us just look at a you just write the numbers that we check, a to the R, a to the 2R, a to the 4R and so on, up to a to the 2 to the S R, these are the elements that we are considering for any a ok. Now, let us look at these numbers R, 2R, 4R and so on.

We will define, what is called as a bad power ok. So, R, 2R, 4R, etcetera are the powers, these are the numbers to which we are raising a. So, bad power the definitions of a bad power is, so say that S is called a bad power; if there exist an x such that x to the S is equal to minus 1 mod n ok. So, look at x to the power s all these computations carried out in mod n; if it is equal to minus 1, then we call this as a bad power ok.

So, in this entire thing we will essentially be working in the group Z n star ok. Z n star consist of all those elements, which are between 1 and n and are relatively prime to n, multiply two elements from there you will in fact get another element in the same collection, and you can do cancellation there that is indeed a group ok.

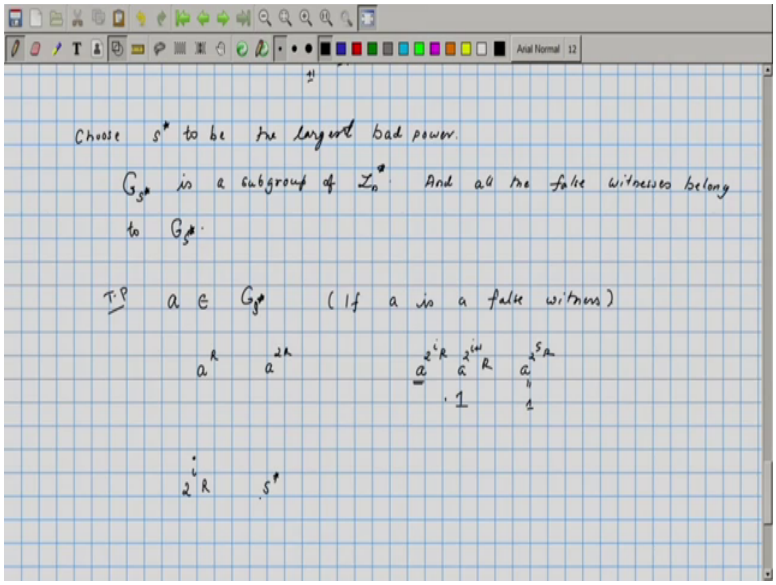
So, we will call a particular element S from these R, 2R, 4R, etcetera as a bad power if you can find an element in Z n star, such that x rays to a S is minus 1 mod n ok. And here is a crucial fact, I will define G S to be this set of all numbers such that so let us say all y such that y to the S is equal to plus or minus 1 mod n ok. So, for any bad power I define this particular collection of sets, they do form a group ok.

So, we have to say that G S is a group under multiplication mod n. In other words, G S is

a subgroup of Z n star ok, how do we verify this? You take any two element in G S, so if you multiply them y 1 y 2 is a product does this belong to G n. So, G S clearly it is a subset of Z n star ok, because we are looking at only those elements y belonging to Z n star, which has this property. So, G S certainly is a subset the elements which from the collection G S is certainly a subset of Z n star.

Now, you take two arbitrary elements y 1 and y 2, if you take that product that is y 1 y 2; y 1 y 2 to the power S is going to be equal to y 1 to the power S times y 2 to the power S, this is equal to plus minus 1 and this is also equal to plus minus 1, the product is also going to be plus minus I mean it is either plus 1 or minus 1 mod n, so that would mean that G S is closed under multiplication, under the group operation. Therefore, G S has to be a any subset which is closed under the operation that has to be a subgroup. So, G S is clearly a subgroup of Z n star. Now, the particular subgroup which contains all the false witnesses, we will define that in a moment.

(Refer Slide Time: 12:38)



So, choose say S star to be the largest bad power. So, we look at all the bad powers amongst them, find the largest that is what we define as S star. Is there even one bad power, only then it makes sense to talk about largest ok.

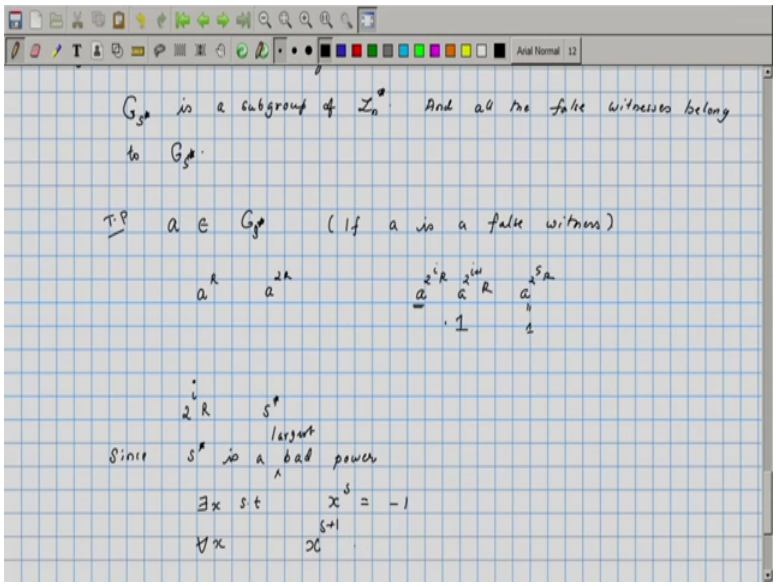
So, we are looking at these numbers R, 2R, 4R, etcetera amongst them, is there at least one bad power. Clearly, R being an odd number is surely a bad power, because minus 1 raised to R is going to be minus 1 ok. So, R clearly is a bad power minus 1 here means 3

minus 1. So, therefore the number R which is an odd number, surely is going to be a bad power; 2R, 4R these are all even number they may or may not be bad powers, but we want to look at the largest bad power, let that be S star.

Now, corresponding to this largest power look at G S star that is going to be a group, this were earlier shown that G S is going to be a group for all possible values of S ok. Therefore, G S star would automatically be a group. So, G S star is a subgroup of Z n star and all the false witnesses belong to G S star ok. Why is this? So, let say a is a false witness ok. So, clearly we need to show that a raised to so if you want to show that a belongs to this particular group, so we need to prove that a belongs to G S star that is if a is a false witness ok.

What we know is a raised to R, a raised to 2R, a raised to the say 2 to the i times R, etcetera. And if you look at this and we have to a raised 2 to the S R, this has to be 1 ok. Now, there is a last point at which so look at the last point that means, there was a 1 ok. So, let us say that was a raised to 2 to the i plus 1 times R, this is 1. And at this point, so let us look at these 2 raised to i ok. So, 2 raised to i and S star which is going to be larger, 2 raised to i times R and S star which of these elements has to be bigger.

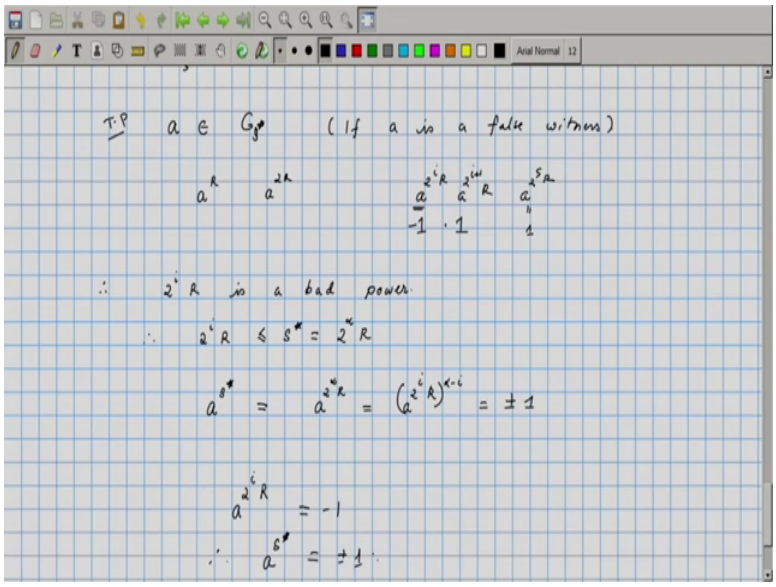
(Refer Slide Time: 16:31)



So, since S star is the bad power ok, we know that so it is a largest bad power. We know that there exist a x such that x raised to S is equal to minus 1, this would also imply that for all x x raised to S plus 1 should be greater than or equal to in this should be this we

will not be equal to minus 1.

(Refer Slide Time: 17:40)



So, we look at the last point at which there was a transition to 1. Since a is a false witness at this point the only number that could have occurred is minus 1 ok, because if it was 1, then of course the last point we assume that the last point at which 1 appears as 2 raised y plus 1, so this not a 1. If it is not a minus 1 that that means, we have found a non-trivial square root of unity. Since both is not happening, we can conclude that a raised to 2 raised to i times R is equal to minus 1. So, therefore we can conclude that 2 raised to i times R is a bad power ok.

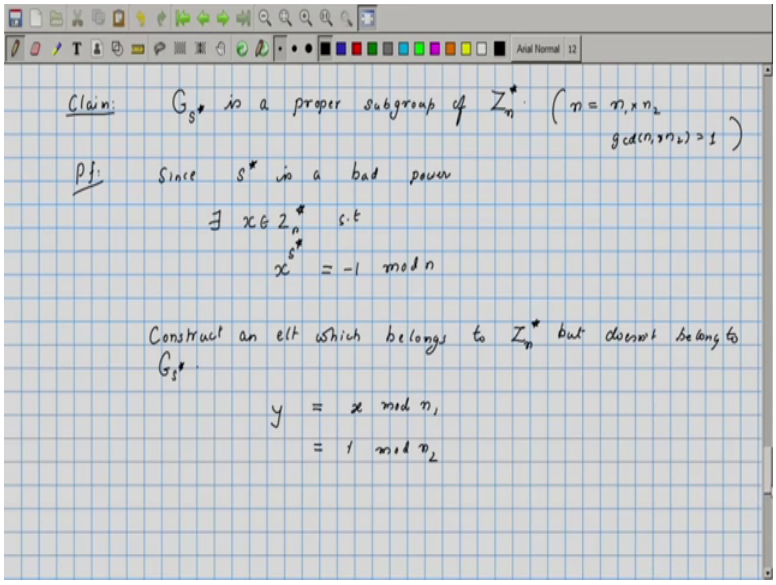
And since a star is the largest bad power, we can conclude the 2 raised to i times R is less than or equal to S star ok. Therefore, if you take a raised to S star that is going to be equal to sorry yeah, if you take a raised to S star, then that is going to be equal to a raised to 2 raised to i times R plus let us say t; t is greater than or equal to 0. And a raised to 2 raised to i ok, and S star is let us assume it is equal to 2 raised to alpha times R. So, this entire thing a raised to S star would be a raised to 2 raised to alpha R, which is equal to a raised to 2 raised to i R the whole raised to alpha minus i ok, so whatever. So, this is coming after 2 raised to i. So, this is going to be equal to plus or minus 1 ok. So, this would imply that a must belong to G S star.

Once again since a raised to 2 raised I mean, a raised to 2 power i times R was the last point at which it transitioned into 1 and is a sequence transitioned into 1. We can

conclude that a raised to 2 raised to i times R is equal to minus 1, this would also imply that since S star comes after this a raised to S mean, so S is a number of the form 2 raised to i times R which comes after i. So, a raised to S star must be equal to plus or minus 1 ok. So, we have now concluded that every false witness must in fact belong to Z n star ok.

Now, what is remaining is to show that we can construct an element, which does not belong to Z n star that means, sorry we can construct an element which belongs to Z n star, but does not belong to G S star ok.

(Refer Slide Time: 21:12)



So, remaining part we will write it as a claim. G S star is a proper subgroup of Z n star ok. So, since S star is the bad power we can conclude that since S star is a bad power, there is an x which belong to Z n star such that x raised to S star is equal to minus 1 ok, so this is minus 1 mod n.

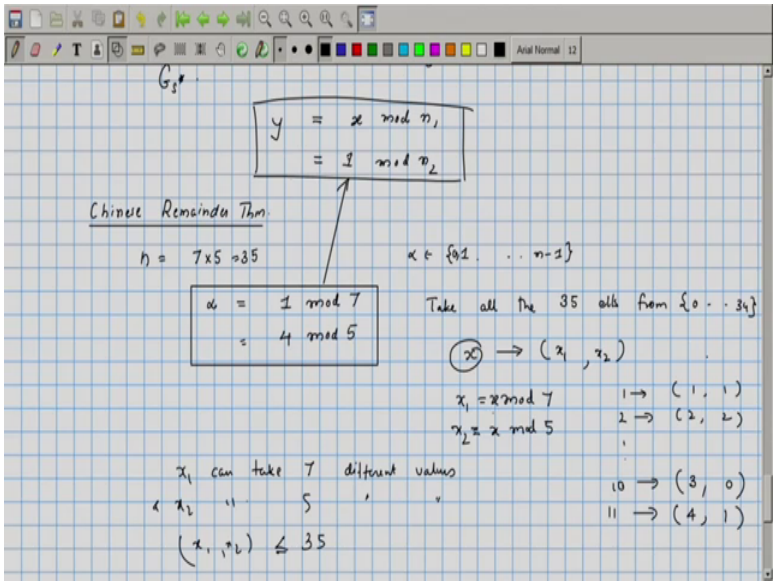
Now, but we can additionally assume here is we are looking at a composite number and that composite number has the feature that it is not a to the power b it is not a perfect power, in particular we can assume that it is not a prime power. So, we can write n as equal to product of two composite numbers n 1, n 2 such that n 1 and n 2 does not have any common factors ok. So, n can be written in this particular way.

So, in order to construct the element, so or proof we will go like this we will construct an

element which belongs to Z n star, but does not belong to G S star ok, so that element will have the following properties we will call that element y. So, y will be equal to x mod n 1 and this will be equal to 1 mod n 2 ok.

So, x is this particular element which shows that S star is the bad power that means, x raised to S star is minus 1 modulo n ok. So, take that x and our y is going to be x mode y is going to satisfy two equations, y should be x mod n 1 and it should be 1 mod n 2, is it always possible to find solution to this kind of equations ok.

(Refer Slide Time: 24:49)



So, it is possible that is what is known as Chinese remainder theorem ok. So, let us see an example of Chinese remainder theorem. So, let us take n is equal to 7 into 5 it is 35 ok. And somebody asked me to find an alpha such that alpha is equal to 1 mod 7 and it is equal to say 4 mod 5 ok. And this alpha must belong to say 1 to n minus 1 that 0 to n minus 1. So, can we find an alpha which satisfies these conditions, our condition here is essentially similar.

We have n 1 and n 2, which are relatively prime they do not have any contact between them. And we are asked to find y between 0 to n minus 1, 0 here will not work. So, we can, because the equation insists that it is 1 mod n 2. So, starting from so you have y some number belonging to Z n star with satisfies this condition. So, in this case y is it possible to always find one such so proof essentially that one can find such is based on the following observation.

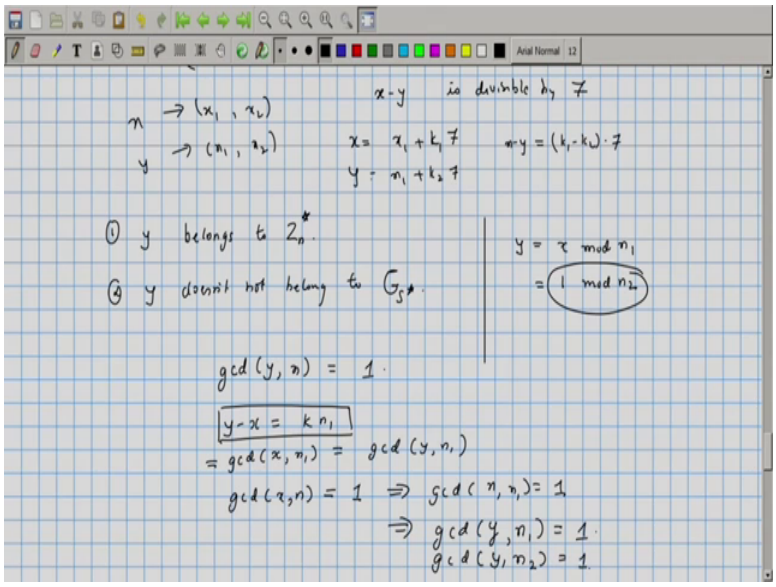
Take all the 35 elements from let us say 0 to 34 ok. So, any element let us say x is being mapped to the following pair ok. So, this is called it as x 1 it is mapped to x 1, x 2; where x 1 is equal to x mod 7 and x 2 is x mod 5 ok. So, every number is basically mapped to a pair of numbers. The first element in the pair being x mod 7 and the second element being x mod 5.

Clearly x 1 can take 7 different values and x 2 can take 5 different values. So, the total number of values at they can together take is less than 35. So, x 1, x 2 the total choices is going to be less than or equal to 35 ok. The so for every number we are doing this for all x, x ranging from 0 to 34 we convert them into pair.

So, for example if you have taken 1 that maps to 1, 1; 2 maps to 2, 2; 10 maps to 3 and 0; and 11 would have mapped to 4 comma 1 and so on ok. So, we are looking at the total numbers of the kind x comma y or x 1 comma x 2 that can appear, maybe we can say that it is no more than 35, but do all the 35 numbers appear.

So, we can say that all the 35 pairs of the form x y, where x is less than x is the x 1 is less than 0 and 6, x 2 is less than x 2 lies between 0 and 4, there are 35 such choices. If we say that none of the pairs repeat, then we can say that everything appears once and exactly once. So, how do we say that none of the pairs repeat.

(Refer Slide Time: 29:03)



So, for example if something here had repeated let us say x 1 x 2 is, so x maps to x 1 x 2

and y also maps to x 1 x 2 ok, what does this mean? If you look at x minus y ok, let us assume x is larger than y; x minus y is divisible by 7 right, because x leaves remainder x 1, y also leaves remainder x 1 when divided by 7. So, x minus y should not leave any remainder ok, because x is equal to x 1 plus k time 7, k 1 time 7 and y is equal to x 1 plus k 2 time 7.

So, if you take the difference x minus y is equal to k 1 minus k 2 time 7 ok. So, we can argue that x minus y is divisible by 7 and we can also argue in the exact same way that x minus y is divisible by 5 ok. The only number between 0 and 34 which is divisible by 7 and 5e was 0 that means, x minus y is equal to 0 ok. So, we can argue that x is equal to y.

In other words, it is impossible the two of them two distinct numbers x and y maps to the same pair. Therefore, every particular pair will be present this means that alpha equals 1 mod 7 and alpha equals 4 mod 5 has a solution in the range 0 to 34. Clearly, it cannot be 0, because 0 would not have given 1, as the remainder mod 7 ok. This proof can be converted into a I mean to a formal proof, where you take two numbers n 1 and n 2 such that n 1 and n 2 multiply and give n and they do not have any common factor between them ok.

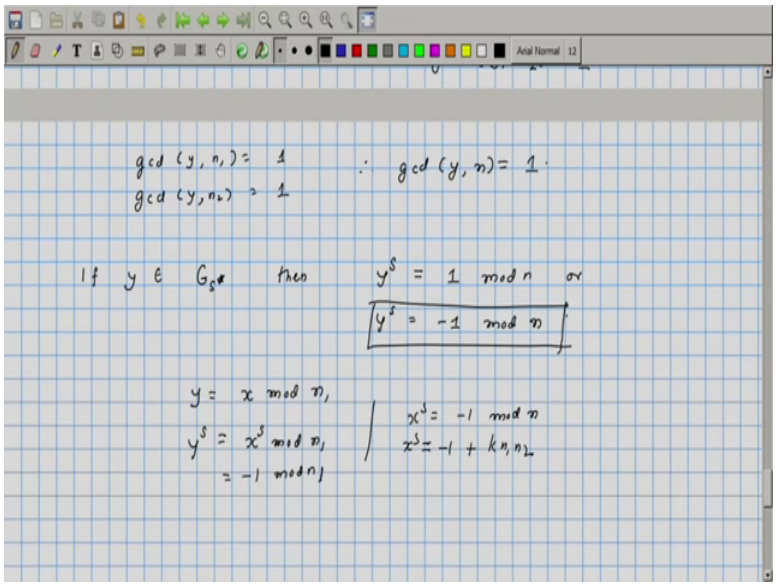
So, we can show that there is one number between 1 and n minus 1, which leaves remainder x when divided by n 1 and remainder 1, when divided by n 2. So, what have we achieved? We have constructed one particular element, but how do we say that this element does not belong to G S ok. We also so we have to show the two things, y belongs to Z n star and the second thing is y does not belong to G S star, these are the two statements that we want to prove. In order to show that y belongs to Z n star, we should show the gcd y, n should be equal to 1.

So, the defining property of y was y is equal to x mod n 1 and this is equal to 1 mod n 2. So, we have this equation that y minus x is equal to k times n 1 ok. So, gcd x, n 1 is equal to gcd y, n 1 ok; because from this equation if x and n 1 had a common factor ok, any common factor of x and n 1, but in fact we have common factor of y ok.

So, gcd x, 1 would be equal to gcd y, n 1; also gcd x n is equal to 1. So, x does not have any common factor with n, because x did belong to Z n star. In particular x cannot have any common factor with n 1, this would imply since gcd x n is equal to 1, this would imply that gcd x, n 1 is equal to 1 that would imply that gcd y, n 1 will be equal to 1 ok.

And from this equation, we can conclude that gcd y, n 2 is also equal to 1.

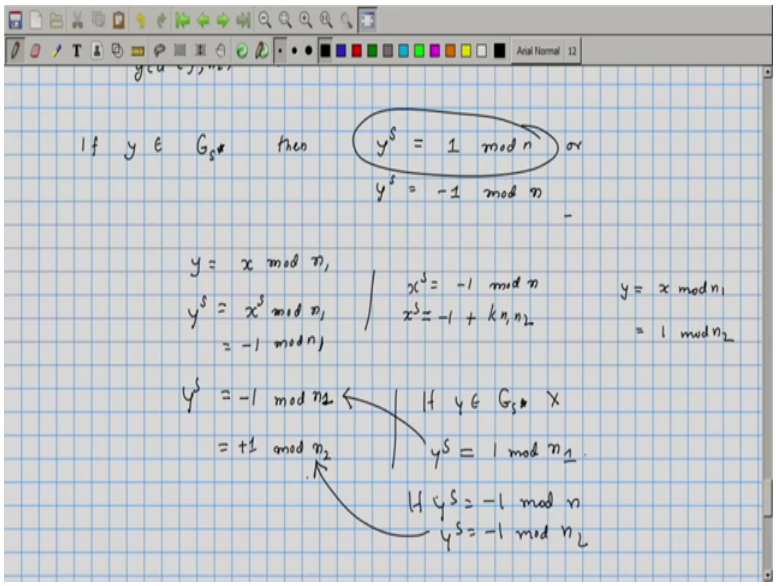
(Refer Slide Time: 34:10)



So, we have argued that gcd y, n 1 equals 1; gcd y, n 2 is equal to 1 that means, y does not have any any common factor with n 1 or n 2. So, therefore gcd y, n is equal to 1 to so we have already managed to show that y belongs Z n star; y does not belong to G S star as what we need to show ok. Now, this is because so if y belong to G S star, then the defining property of G S star is y raised to S is equal to plus 1 mod n or y raised to S is equal to minus 1 mod n ok.

But, r y has this property that it is equal to x mod n 1. So, if you take y raised to S that will be x raised to S mod n 1 and this has to be equal to minus 1, because x raised to S is equal to minus 1 mod n. So, x raised to S is equal to minus 1 plus k times n 1 n 2. So, this would imply that x raised to x is equal to minus 1 mod n 1 ok; so, this is minus 1 mod n 1 ok.

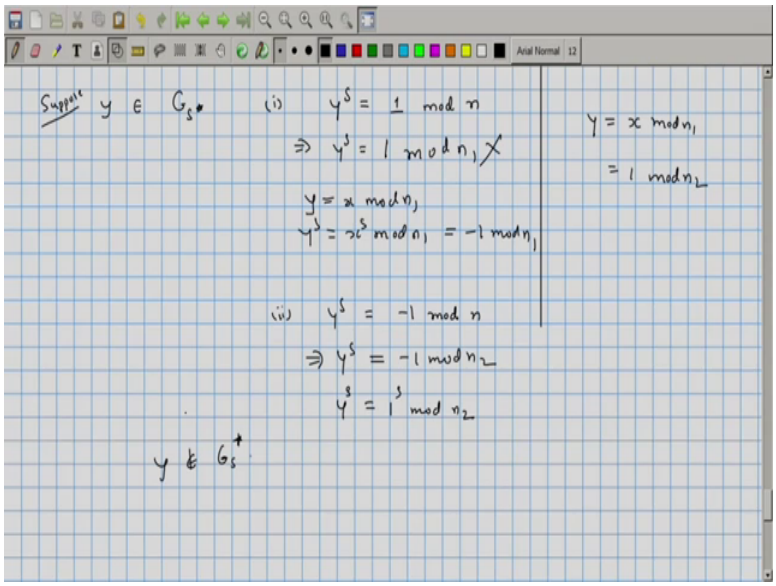
(Refer Slide Time: 35:54)



So, clearly this is the only possibility. So, y raised to S is minus 1 mod n 1 and y raised to S is equal to 1 mod n 2. So, the defining equation for y was y is equal to x mod n 1 and this is equal to 1 mod n 2. Therefore, y raised to S is equal to 1 mod minus 1 mod n 1 and it is equal to plus 1 mod n 2 ok. So, let us say if y belong to G S star and if this condition is true, y raised to S is equal to 1 mod n 1. Then we can conclude that y raised to S is equal to 1 mod n 1 as well, but that will directly contradict with this, so this is not possible.

If y belongs to G S and y raised to S is equal to minus 1 mode n n, then we can say that y raised to S is equal to minus 1 mode n 2 and that will contradict with this condition ok. So, in either case we get a contradiction ok.

(Refer Slide Time: 37:14)



So, once again suppose y belongs to G S star. There are only there are two cases, so case one y raised to S is equal to 1 mod n ok, and the case two would be y raised to S will be minus 1 mod n, but our y had the following properties or y had the following properties y is equal to x x mod n 1 and it is equal to 1 mod n 2.

If y raised to S was 1 mod n 1, this would imply that y raised to S is equal to 1 mod n 1 as well ok; but since y is equal to x mod n 1, we have y raised to S is equal to x raised to S mod n 1, but x raised to S was minus 1, so this is minus 1 mod n 1 that contradicts with this. If y raised to S is minus 1 mod n, in that case y raised to S is also this would imply that this is equal to minus 1 mod n 2. If y raised to S is minus 1 mod n 2 that directly contradicts with y equals 1 mod n 2, because it is raised both sides to power S, we will get y raised to S is equal to 1 mod n 2.

So, in either case we get a contradiction, so that would mean that y does not belongs to G S star, so that essentially means that the set of all false witnesses, they form a subgroup. And since a subgroup is at most half the size of Z n star, Z n stars maximum size is n minus 1, therefore you cannot have more than 50 percent of the elements as false witnesses. Therefore, our algorithm has more than 50 percent chance of success in each run. So, repeat the algorithm as many times as you want the; I mean depending on the probability of success that you are happy with.