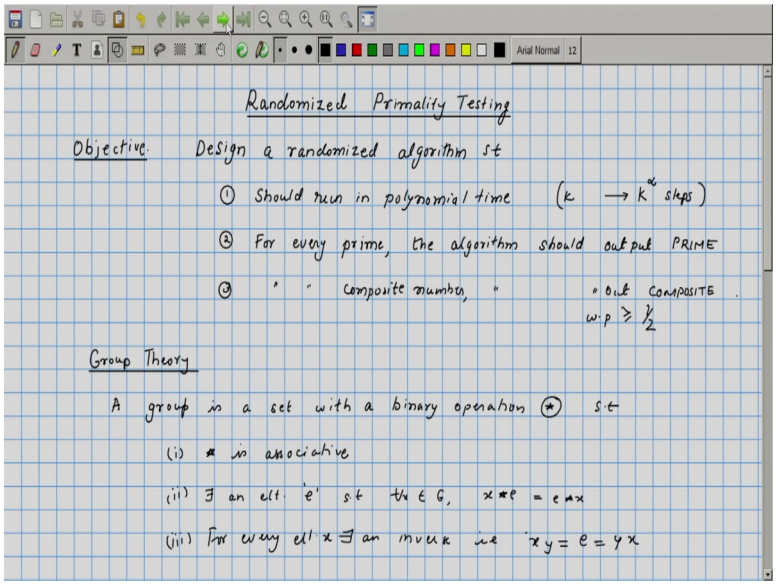
Randomized Algorithms
Prof. Benny George Kenkireth
Department of Computer Science & Engineering
Indian Institute of Technology, Guwahati

Lecture - 24
Primality Testing

(Refer Slide Time: 00:30)



In today's lecture we will learn about Primality Testing, our objective is the following, so design an algorithm a Randomized Algorithm, such that first should run in polynomial time; that means, of the input as of size. Let us say k then the algorithm should take no more than k raised to alpha steps for some fixed alpha.

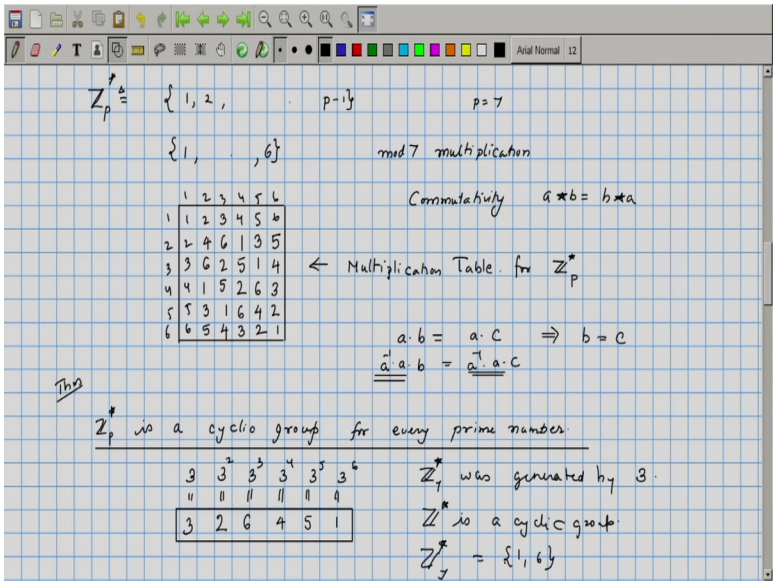
The second requirement is for every prime, the algorithm should output prime ok. And for every composite number the algorithm should output composite with probability greater than half ok. So, this probability is over the random choices that the algorithm mix; and this should be true for every composite number ok.

So, we will use some elementary principles from group theory, so let us initially understand what is a group? So, a group is a collection of mathematical objects you can call it as a set with binary operation let us say we call it a star such that, first star is associative so since it is an binary operation we will assume closure it is for any 2 elements in the set.

If you combine them using star, use the resultant element will be a element of the group. Second there exists an element e or identity such that for every x belonging to g x star e is equal to e star x. And the third requirement is for every element there exist an inverse that is there is an element y such that xy is equal to identity that is equal to y times x as well ok. So, if binary operation which is these 3 properties is essentially called as called a group.

So, you can think of groups as mathematical structures wherein you can multiply and divide ok. So, if you call the operation as multiplication you can call it by whatever name you can call it addition, multiplication whatever is the binary operation you can essentially multiply and divide that inverse operation you can perform ok.

(Refer Slide Time: 05:13)



So, let us see an example the example that we would require, so this will be called as Z p, so let us say p is a prime number and if you look at numbers 1 2 up to p minus 1 ok. So, let us say p equal 7; then this will be these numbers from 1 to 6 of course, if you add 5 and 6 you will get 11, but that is not 1 of the elements of Z p ok.

But here the operation we are going to redefine it. So, we will have mod 7 multiplication ok. So, we can just represent this entire thing by a table ok. So, 1 2 3 4 5 6 1 2 3 4 5 6 are the elements 1 2 1 that will be 1 so mod 7 as well. So, this is a special group which is an additional property of commutativity ok.

So, we will say that a group is commutative if a star b is equal to b star a, the order does not really matter 2 into 2 is 4 2 into 3 is 6 2 into 4 is 8 which is 1; 2 into 5 is 10 which is 3 mod 7 this is 5; so you can just fill up the elements of this group 3 4 is 2 5 ok. So, this will be the multiplication table for this particular group since it is under multiplication we will just Z star p.

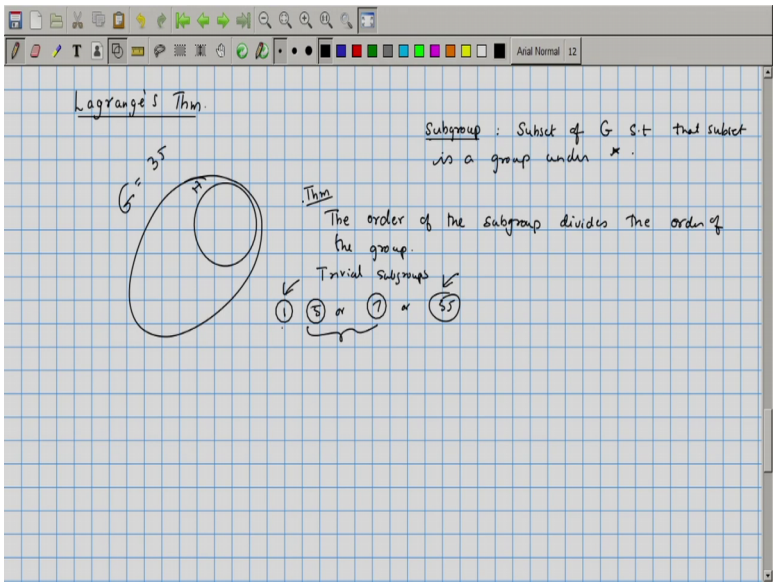
Now, you can see that this particular operation has many nice properties, each row is a permutation of 1 to 6 and we can take this operation and do multiplication as well as division that is if you have let us say a times b is equal to a times c we can write we can basically apply cancellation. So, this would imply that a equals c sorry apply that b equals b equals c because we can just multiply both the sides with a inverse. So, inverse times a times b this is equal to a inverse times a times c.

So, this gives you identity this gives you identity times anything is going to be identity. So, from all these rules we can conclude that b must be equal to c. So, we can basically do cancellation; so that is a group and Z p star so there is a theorem Z p star is a cyclic group for every prime number ok. For example, if you so cyclic group means it can be obtained by taking some particular element and multiplying with itself.

So, here if you take the number so let us try, if you take the number 3 3 square is 9 that is 2. So, let us compute 3 3 square 3 cube 3 raised to 4 3 raised to 5 and 3 raised to 6. This is equal to 3 this is equal to 9 which is equal to 2, and this is 2 into 3 that is going to be 6 and this is going to be equal to 6 into 3 that is 18 that is 4 12 this is equal to 5 and 5 into to 3 is 15 which is equal to 1.

So, you can see that the entire group all the elements in the group were generated; so Z star 7 was generated by 3. So, therefore, Z star 7 is a cyclic group ok. So, this is not in general true for an arbitrary group, but for every group which is obtained from a prime number in this format is going to be a cyclic group ok. So, this is a theorem that we will need, and also require a couple of other theorems.

(Refer Slide Time: 11:45)

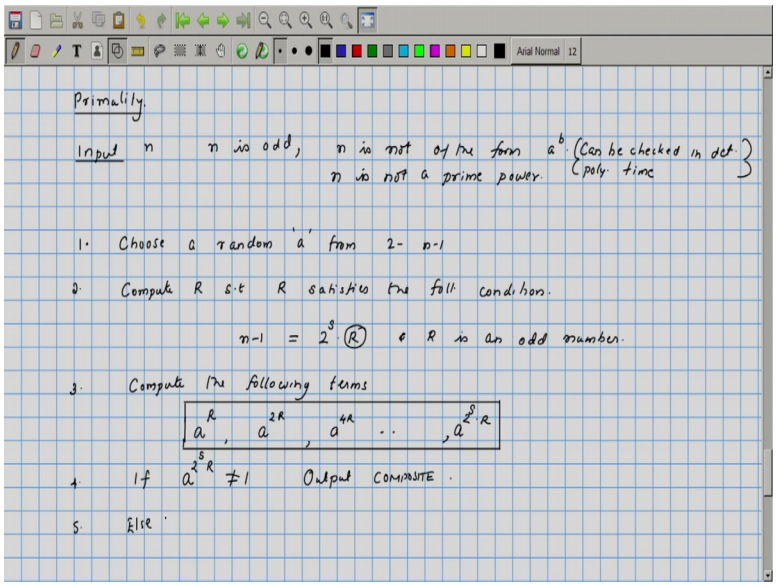


The next theorem that we will use is called Lagrange theorem ok; so this states that so suppose this is this group, and let us say this is a sub group sub group is a you need to define what is a sub group? Sub group is a sub set of the subset of G such that that subset is a group in its own right under the same operation, let us say G was a group under star if you find a subset which is a group under the operation star that will be a sub group.

So, if you look at the; if you look at this group Z star 7 and if you take the numbers let us say 1 and 6 you can verify that this is going to be a sub group of Z star 7. So, Lagrange theorem says that, the order of the group divides the order of the sub the order of the subgroup divides the order of the group which essentially means so if G had 35 elements; any subgroup must have either 1 element or 5 or 7 or 35 elements ok.

These subgroups are essentially are I mean these are called the trivial subgroups, because 35 element subgroup is a group itself and the single element subgroup is going to be the group which consists of just identity element; so, these are non trivial subgroups ok. So, these are the theorems that we would require and there are some additional results that we would need, but we will derive them on the fly ok.

(Refer Slide Time: 14:33)



So, now let us look at primality; so we were given a number n ok, we will assume few things about n first we can assume that n is odd next we will assume that, n is not a prime power that is it is not of the form p power ok. So, we will assume that p is not n is not a not of the form a to the power b this can be easily checked ok, for any input is it of the form a to the power b this can be checked in polynomial time deterministic polynomial time ok.

So, once we have completed these checks for the input, we can assume that n is odd and n is not of the form e to the power b particular n is not a prime power ok, and our algorithm the steps of the algorithm are as follows. So, choose a random a from 2 to n minus 1, so compute R such that R satisfies the following condition; n minus 1 should be equal to 2 power S times R and R is an odd number.

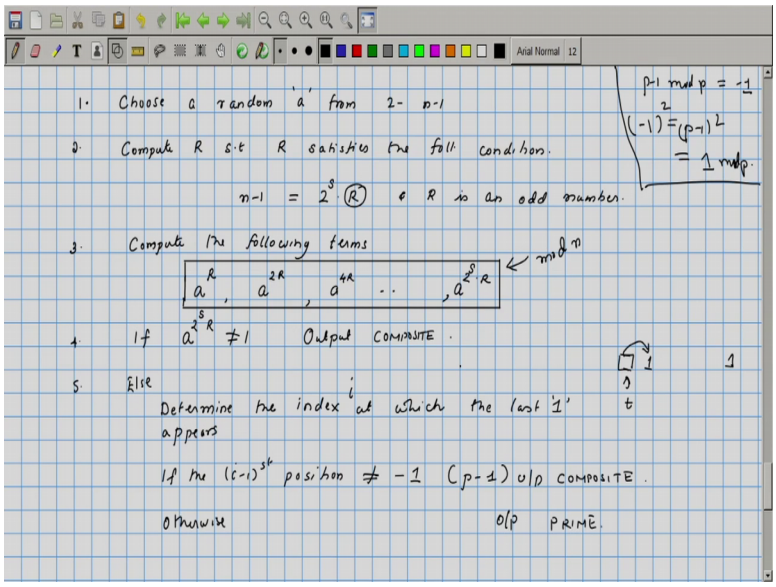
So notice that this can be done only in one particular way, for any number you just take out all the powers all the even all the powers of 2 from it and whatever remains that is what we call as R ok. And this can be this can of course, be done in polynomial time and since n is an odd number n minus 1 is going to be an even number; so R certainly is less than n minus 1 and then we will compute the following compute the following terms.

So, we will first compute a to the R and then a to the 2 R a to the 4 all the way up to a to the so we keep on repeatedly squaring the numbers that we have obtained these are all a

to the R squared will give a to the 2 R and that squared will give a to the 4 R and then finally, we will get a to the 2 to the S times R ok.

Now, a to the 2 to the S times R should be equal to 1 why so? Well it depends on whether n is prime or not. So, we will compute these and then based on the values that we have obtained here; so these values we will look at it more carefully, and based on these values we will conclude whether the number as prime or composite.

(Refer Slide Time: 19:39)



So, if a to the 2 to the S times R is not equal to 1 we will output composite. So, if that is not so else, if so in that case a to the 2 to the S R is going to be equal to 1. So, if the so if the last term is going to be 1 in the other cases ok, maybe there are 1s before that ok, but there is a last stage at which, I mean last position at which a number which is not 1 when squared gave you 1 look at that position ok. So that position let us call it as t.

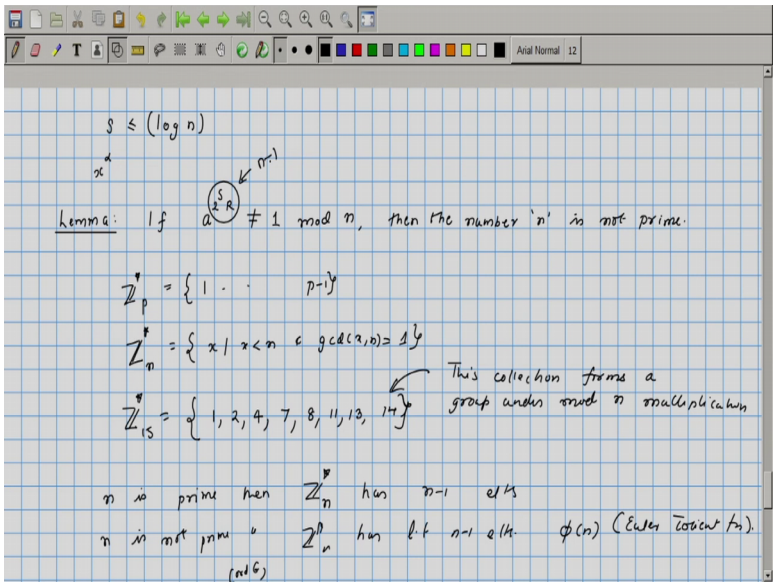
So, we will say else we will determine the index at which the last 1 appears ok. So, let us call this as the index i and if the i minus first position is not equal to minus 1 so minus 1 here means the number p minus 1. So, these squaring operations we are carrying that out in mod mod n all these operations we are carrying out mod n and if the i minus first position was not equal to minus 1.

So, minus 1 is the equivalent of p minus 1. so p minus 1 mod p we will we can just write it as minus 1 or minus 1 as a symbol for p minus 1 ok; and notice that minus 1 squared

will is essentially p minus 1 the whole square you can verify that that is going to be 1 mod p ok. So, if this is the case if this is not equal to minus 1 then we will declare composite and otherwise declare prime, so otherwise output prime so this is our algorithm ok.

So, there are 2 places where the algorithm outputs composite, and if it does not output composite the output is going to be prime. So, now, we need to argue that this algorithm has the correctness requirements that we had initially mentioned; clearly there are algorithm runs in polynomial time because all these calculations this is S repeated squarings and S is so S is less than say log n.

(Refer Slide Time: 22:50)



So, when we talk about polynomial time we want to mention, that the algorithm works in polynomial time no I mean so the input size is x then the algorithm works in x to the power alpha at most it does not take more than x to the power alpha for any input of size x ok.

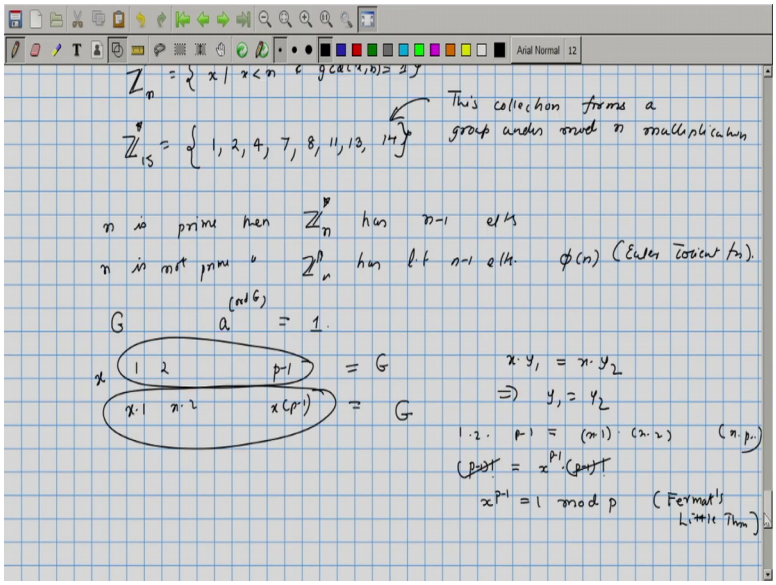
So, here if an n bit binary string as being given or an n bit decimal number as given the input size is log n ok. And so we want the algorithms running time to be log n to the k for some fixed k ok. So, here all these operations S is at most log n so we have only log n multiplications and each the numbers involved are between 1 and log n between 0 and log n. So, all those operations can be carried out in polynomial time.

Now, let us look at the cases where it is declaring the number as composite ok. So, first is when a to the 2 to the S R not equal to 1 so we will write this as Lemma if a to the 2 to the S times R is not equal to 1 mod p, mod n then the number n is not prime by is this so well; we define the set Z star p consisting of all elements from 1 to p minus 1. We could also write this set Z star n minus or n for an arbitrary number n which consists of all x such that x less than n and g c d x n is equal to 1.

So, take all the numbers which are relatively prime to a number and collect them in a basket, and allow the multiplication operation to be mod n multiplication you can check that that will in the form a group. For example if you take Z star 15 this will consist of the following elements 1 2 4 7 8 11 13 and 14. So, there are 8 elements here and you can verify that, this collection forms a group under mod n multiplication ok.

So, Z star n is always a group, so you can do the operations there, but note that if n is prime, then Z star n has n minus 1 elements and if n is not prime then Z star n has less than n minus 1 elements. In fact the number of elements there will be given by the Euler Totient function ok.

(Refer Slide Time: 27:02)



So, whenever n is prime this is this group has n minus 1 elements, and other words it has less than n minus 1 elements and we can show that if you take any group any finite group G and you take any element a a to the number of elements. So, we will denote it by order

G this is going to be equal to 1 ok. Why is this so? We will just show this for commutative groups our group is anywhere commutative.

So, take all these elements 1 2 up to p minus 1 ok, now when you multiply this with an arbitrary element let us say x you will get x times 1 x times 2 x times p minus 1 ok; now this collection as a set is going to be exactly equal to G; this is anyway equal to G and this is also going to be G because all these products are going to give you distinct elements it is x times y 1 is equal to x times y 2 implies y 1 equals y 2 we can apply cancellation ok

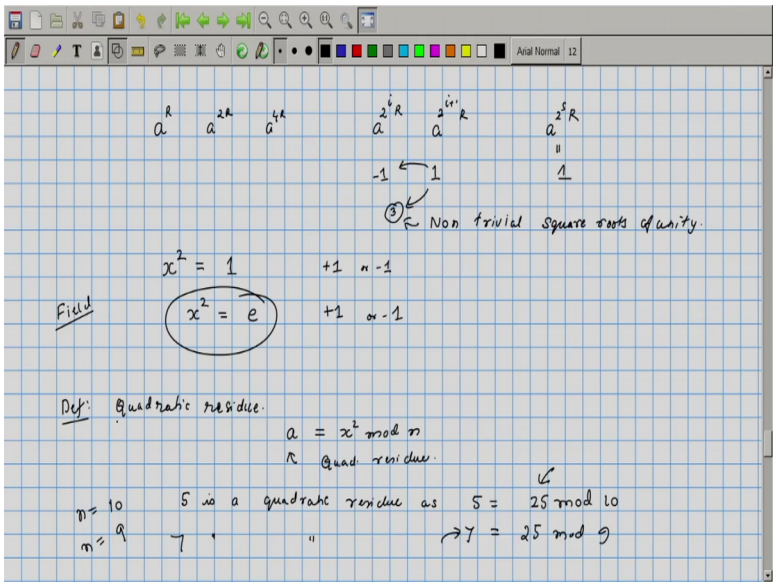
So, if you take distinct elements y 1 and y 2; you will get distinct products x y 1 and x y 2 ok. So, there are going to be p minus 1 elements here all of them being distinct, so that has to be exactly the group G. So, we can write 1 so if you take the product of all the elements 1 2 up to p minus 1, that is going to be equal to x times 1 times x times 2 times x times p minus 1 ok.

So now you can just cancel off things can rearrange, so this v if you write it as p minus 1 factorial this is going to be equal to x raised to p minus 1 times p minus 1 factorial all these operations carried out mod mod mod p minus 1 or mod n so these gets cancelled. So, we will get x raised to p minus 1 is equal to 1 mod p this is also known as, so this result when applied to Z p star is also known as Fermat's little theorem ok.

So, what we know is, when the number is prime it has to be the case that x raised to p minus 1 should be equal to 1. So, if it is not 1 then we can readily declare it as composite ok; and 2 raised to S times R is nothing but n minus 1 ok; so if this is not equal to 1 then the number is not prime and therefore, we are correctly declaring it as composite.

Now, let us look at the second instance where we are declaring it as composite; we checked at the last index from where there was from where the sequence of 1s it began ok; 1 before that that index if a number other than 1 appears other than minus 1 appears then we had declared it as composite ok.

(Refer Slide Time: 30:32)



So, let us look at this more carefully so we had computed a raised to R a raised to R a raised to 4 R and let us say a raised to 2 to the i R and then a raised to 2 to the i plus 1 R all the way up to a raised to 2 to the S R this has to be 1, and if a 1 appears at any place it is square is also going to remain as 1 of course, if a minus 1 appears at some place at the next place the minus 1 squared is going to give you 1.

So, if you look at the last 1 the position before it could be either a minus 1 or it could be something else as well ok. If it is some other number let us say this 3, then we would have declared it as composite why is this a correct thing to do. So, these will be what we will refer to as non trivial square roots of unity or square roots of unity ok.

So, if you look at the equation x square equals 1 this is precisely 2 roots when we are talking about real numbers plus 1 and minus 1. We could in a general in an algebraic structure known as a field we could look at the equation x square equals identity ok. And or so in this case there I mean if it is a field there can be precisely 2 roots plus 1 and minus 1.

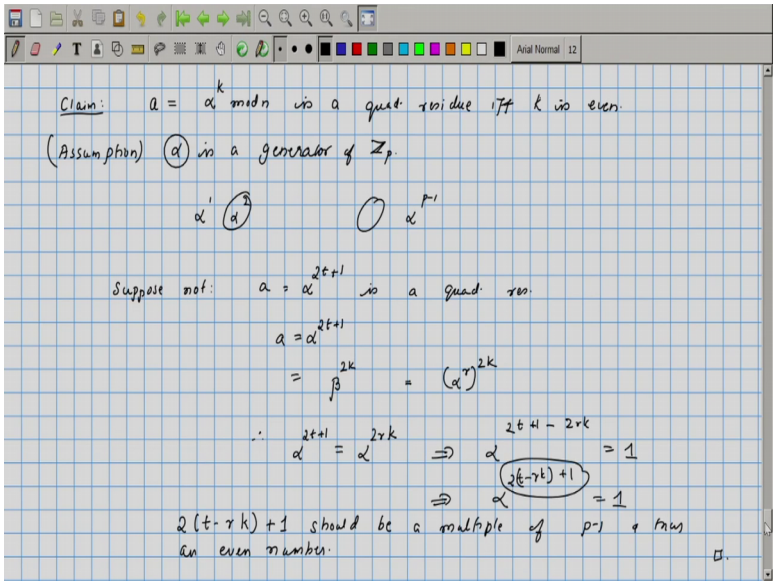
So, here we have a case of we need to first show that the algebraic structure that we are working with is in the other field, and then what we have essentially found is a non trivial square root of unity. And if the algebraic structure that we were working with happens to be derived from a prime number that is going to be a field and for non primes it is not going to be a field.

So, that is the essential idea behind why we are declaring the number to be composite when we see a non trivial square root of unity. So, let us try and prove this using more I mean simple number theoretic arguments. So, let us just look at this equation. So, we will define what is called as a quadratic residue ok. So, if a is equal to x square mod n ok, then we will say that a is a Quadratic residue ok.

So if you take for example, n equals 10 and if you take the number 5; 5 is a quadratic residue, so 5 is a quadratic residue as let us say I mean 5 is equal to 25 mod 10; then this is the square. It so happens that it is square of 5 itself, but let us say I mean if we had taken n equals say 9 and in that case we can say that 7 equals 25 mod 9 therefore 7 is a quadratic residue ok.

So, any number which you obtain by taking the remainder when you divide a square that is take a number multiply in to itself whatever mean the group, and compute the remainder mod n, number that you get is what is called as a quadratic residue.

(Refer Slide Time: 35:23)



So it is a claim, exactly half so we will prove the following statement so a equals say alpha to the power k mod n is a quadratic residue if and only if k is even ok. So, here I am assuming that alpha alpha as a generator of let say Z p ok. So, we are looking at the group consisting of 1 to p minus 1 and in this particular group, let us say alpha is a generator and we are looking at all numbers so since alpha is a generator the different

elements will be alpha alpha square alpha raised to p minus 1 p being an odd prime it is going to be I mean p minus 1 is going to be an even number.

So, here we are saying that all these quantities there I mean these quantities are going to be quadratic residues well one thing is clear these will be quadratic residues because they are alpha raised to some 2 to the power 2 times k which can be written as alpha raised to k the whole square. So, when you go mod n whatever you get that is by definition of quadratic residue; but what we want to argue is that these alone are quadratic residues and there are no other quadratic residues how do we say that?

So, suppose not ok; that means, alpha to the let us say I mean 2 t plus 1 for some t is a quadratic residue. Therefore, mean let us say this is equal to a we can write this as alpha 2 t plus 1 mod n which is equals so a I mean whatever is your a; a is equal to alpha raised to 2 t plus 1 mod n that is a perfect square right. I mean this alpha 2 t plus 1 is a perfect square, so that is some beta raised to 2 k all these so we will not write mod n because all these things are carried out in mod n.

So b to the so a can be written as b to the 2 k and since it is beta to the power 2 k we can write since this is a cyclic group beta itself is going to be alpha 2; let us say some power r times 2 k. Therefore, we can write alpha to the 2 t plus 1 is equal to alpha to the 2 rk now this implies that alpha to the 2 t minus so 2 t plus 1 minus 2 r k is equal to identity this would imply that alpha to the 2 t plus 1 2 times t minus rk plus 1 is equal to identity ok.

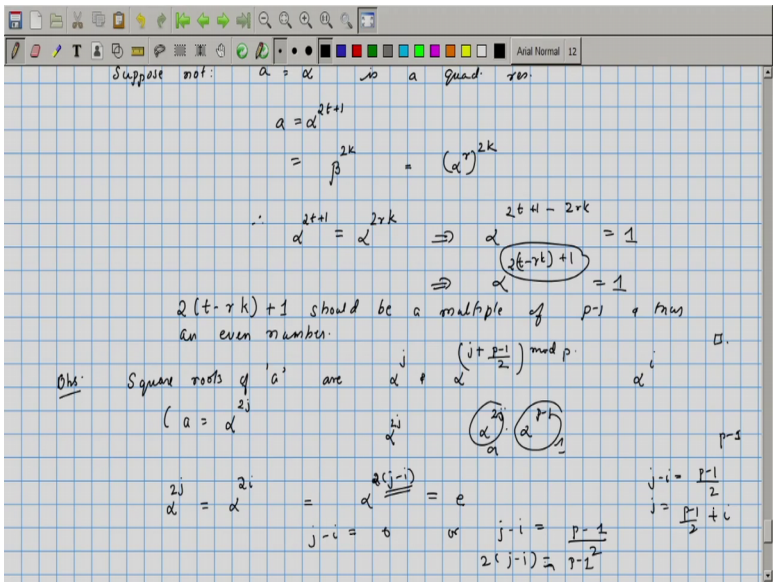
But if alpha to the to some power is identity ok, the smallest number which has this property that alpha to the let us say it I means say capital T is equal to identity means T should be a multiple of p minus 1. If it is anything smaller than p minus 1 that means, alpha does not generate I mean alpha does not generate the entire group. And if it is something which is not a multiple then we can take the remainder of I mean let us say alpha to the T equals 1 take T mod p minus 1 alpha so let us call this as T prime alpha to the T prime will also be equal to 1 ok.

So, we can say that this number 2 t minus rk plus 1 should be a multiple of p minus 1 any multiple of p minus 1 is an even number, but this is an odd number. So, this is not just possible ok. So, we can just write this down as the following 2 times t minus r k plus 1

should be a multiple of p minus 1 and thus an even number so that will give us the required contradiction ok.

So, every quadratic so we can say that if it is a if any number is a quadratic residue, then alpha to the k that k should be even. And this would also mean that the square roots of a so we can write this as an observation. So, by square roots a we mean those numbers which when squared modulo n gives a are going to be alpha to the power 2 j ok.

(Refer Slide Time: 41:51)



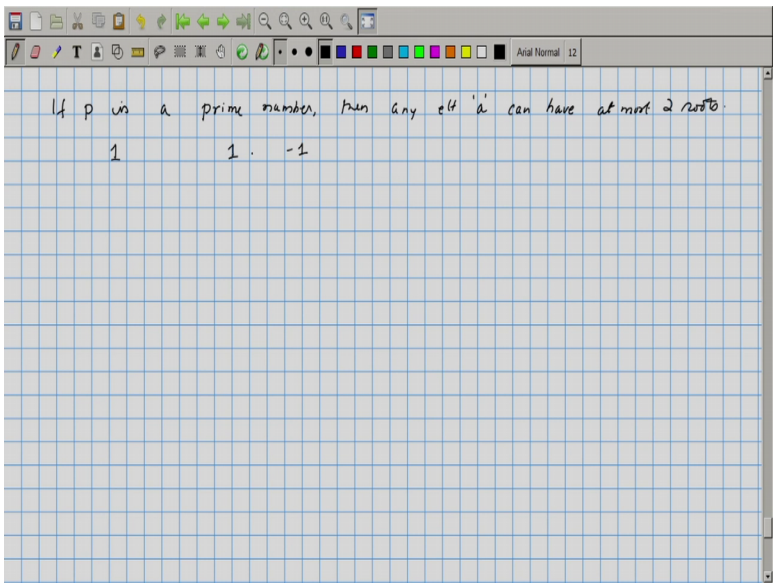
So, we can write the square root says alpha to the j and alpha to the j plus p minus 1 by 2 so you can think of this mod p p being an even odd number p minus 1 by 2 is going to be a an integer that plus j. So, alpha j is 2 j if you square it you will get a and if you square alpha to the power j plus p minus 1 by 2, there also you will get alpha to the 2 j times alpha to the p minus 1 alpha to the p minus 1 is going to be 1 this is going to be a.

So, these are going to be the square root and there cannot be any other square root because you can say that if there was any other square root alpha to the power i ok, then we will get so let us see what goes wrong; if alpha to the i is a square root of a then alpha to the j so alpha to the 2 j is equal to alpha to the 2 i ok. And since these are equal we can conclude that alpha to the 2 times j minus i should be equal to identity it should be equal to 1 and therefore, j minus 1; so, what are the possibilities?

So, j minus i should either be 0 or j minus i should be equal to p minus 1 j minus i equals p minus sorry j minus i should be p minus 1 by 2 only then 2 times j minus i will be equal to p minus 1. This cannot be any other multiple because 2 times j minus 1 cannot be as largest let I mean j minus i is at most as big as p minus 1 it is it is going to be definitely smaller than p minus 1 therefore, 2 times p minus 1 cannot be larger than p minus 1.

Therefore we can conclude that 2 times j minus i must be equal to p minus 1 and this would tell us that i is going to be equal to j yeah. So, j plus p minus 1 or j minus p minus 1 does not really matter mod p so this will tell us that j minus i is equal to p minus 1 by 2 or j is equal to p minus i by 2 plus i. So, there are only 2 possibilities essentially; so you can have precisely I mean if p was a prime number; it can have at most 2 roots of unity and we know that those roots i mean it can any number can have it at most 2 roots.

(Refer Slide Time: 45:16)

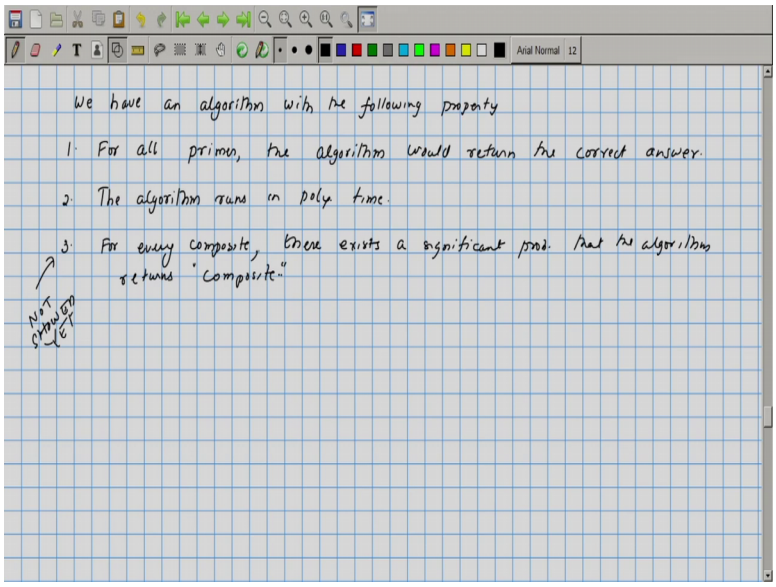


So, if p is a prime number, then any element a can have at most 2 roots ok. So, in particular if you take the element 1 it can have only 2 roots 1 and minus 1, because these are anywhere roots it cannot have any additional roots when we find the number which satisfies this condition that is it is a non trivial square root of unity then we can declare it as composite ok.

So, what we have concluded is the following whenever this algorithm declares the number as composite there is a sound reason; I mean it is never incorrect on that count

ok. It is always correctly declaring the number as composite whenever it declares it as composite; it does not make a mistake in that. Whereas, whenever it declares a number as prime things could go wrong we will check with what probability things could go wrong.

(Refer Slide Time: 46:43)



So, let me just summarize whatever we have done so far; so we have an algorithm with the following properties. First for all primes the algorithm would return the correct answer; this is because what we had argued is that for every composite number I mean whenever the algorithm declares as a number as composite it is never a prime number ok.

So, that would essentially mean that whenever the algorithm declares the answer as whenever the algorithm gets an input as a prime number it cannot declare that as composite, and hence for all primes the algorithm must return the correct answer. The second thing that we have that our algorithm we have checked is the algorithm runs in polynomial time what we need to verify is that, for every composite there exists a significantly high probability this is this we have not showed yet probability that the algorithm returns composite outputs composite ok.

So, let us see what happens for a composite number ok, so we had randomly chosen a number from 2 to n minus 1 ok. So, the numbers which will then the choices of a which will result in the number being declared as composite; we will try to bound that set, but

we will show is these a's which will make the number a composite number or the as which will bear testimony to the compositeness of the number n will essentially be significant collection of means significant subset of 2 to n minus 1.

To show this what we will indeed prove as the numbers which do not which bear false testimony, will essentially form a group it will form a strict subgroup of the set Z n star since it is a subgroup of Z n star it is size is surely less than half of the size of the total elements in Z n star. So, that will surely be less than n by 2 and I mean that is by Lagrange theorem and that we will basically conclude our proof that is the part we will do in the next class.