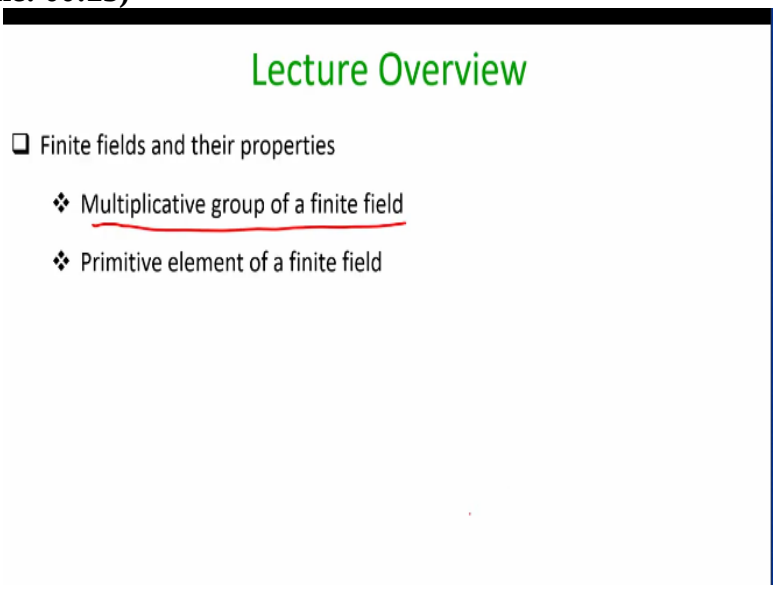
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology, Bangalore

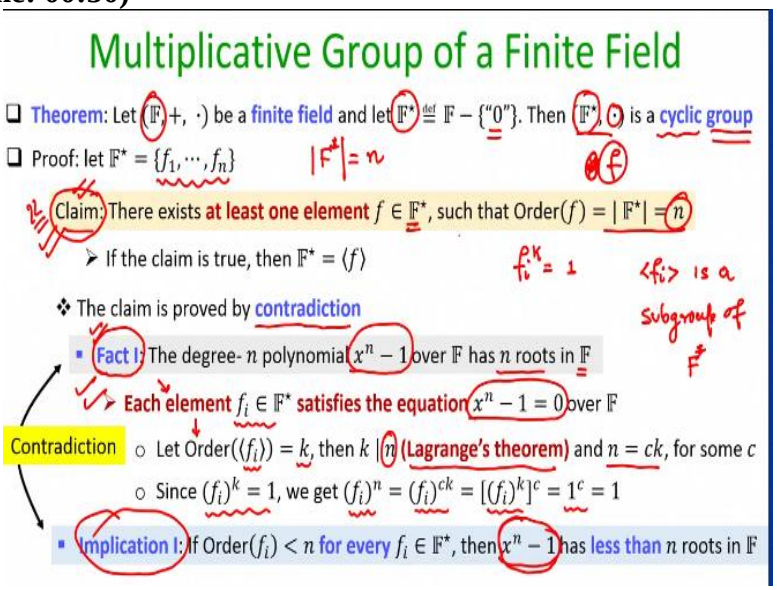
Lecture – 70
Primitive Element of a Finite Field

(Refer Slide Time: 00:23)



Hello everyone, welcome to this lecture, in this lecture, we will continue our discussion over finite fields and we will focus in this lecture on the multiplicative group of a finite field and we will prove some nice properties regarding the multiplicative group of a finite field specifically we show that it is always a cyclic group, it will have some generators and those generators are called as the primitive element.

(Refer Slide Time: 00:50)



So, let F be a finite field with an abstract plus and dot operation and I denote by F* the set consisting of all elements of the field except the 0 element where 0 is the additive identity

element. And my claim here is that if I focus on the nonzero elements of the field and dot operation, then that constitutes a cyclic group. And of course, it constitutes a group that comes from the properties of your field axioms.

But what I am claiming here is that it is actually a cyclic group and by cyclic group, I mean that has at least 1 generator. That means, there exists at least 1 special element g or say f here such that all the different powers of f will give you the elements of this set F*. So, the proof strategy here will be the following, so basically I want to show the following: imagine that the nonzero elements are f_1 to f_n, there are n such elements.

My goal is to show the following, I am claiming here that there exists at least 1 element f in this collection F* whose order is n. By that I mean that f^n is your identity element and n is the smallest such positive integer. If I can show that this claim is true, then that shows that indeed my set F* constitutes a cyclic group. It is already a group as I said, but if this claim is true, I end up showing that it is actually a cyclic group.

And the proof is slightly involved we will be taking help of several lemmas which are actually independent properties of groups and so on. And then we will finally arrive at the proof of this claim, so the claim is actually proved by contradiction. So, we want to show that there exists at least 1 element in this collection F* whose order is n, the contradiction will be that there exists no element in the set F* whose order is n, that is a contradiction.

If that is the case, then I have to arrive at some contradiction or some false statement. So, the proof strategy will be the following. I will be taking help of a simple fact regarding polynomials over the field. My fact here is the following, my claim is that if I take this degree n polynomial which is a monic polynomial over the field, then it has exactly n roots in the field F. That is my fact 1, I will very I can prove this very easily, but this is my fact.

Actually if you see; if you recall the properties of the roots of polynomials, we know that since the polynomial here has degree n, the number of roots can be at most n, but my fact here is that it has exactly n roots from the field F and the proof of this fact is the following. My claim is that you take any element from the set F*, that means you take any nonzero element from the field F it will satisfy this equation ($x^n - 1 = 0$).

If that is the case, then basically I am showing you that all elements of set F* are actually the roots of this equation or roots of this polynomial. So, let us prove this fact that each element of the set F* is a root here. So imagine that the order of the element f_i is k. By that I mean that the number of distinct field elements which I can generate by computing different powers of f_i is k; that is another equivalent definition of an order. That means f_i^k is your identity element.

Now I can invoke here the Lagrange's theorem of groups and subgroups. Since this cyclic subgroup $<f_i>$ is a subgroup of your parent group F*, of course, with the dot operation that I am not writing down separately, then as per the Lagrange's theorem, the Order($<f_i>$) or the order of cyclic subgroup $<f_i>$ generated by f_i should divide the order of your parent group and the order of the parent group is n because as per my definition F* cardinality is n.

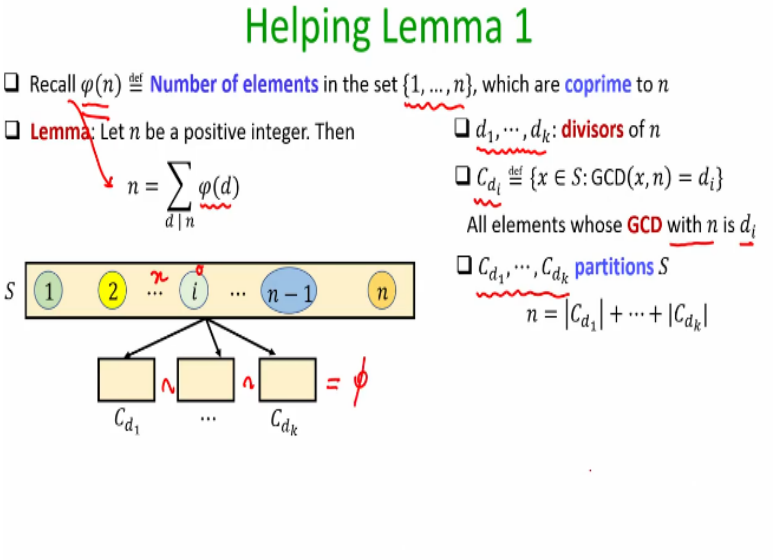
So, n is divisible by k that means, n can be written down as some c times k. That means, I can say that, since f_i^k is 1, then f_i^n will give me the same element which I obtain by raising $(f_i)^{ck}$. Then as per the rules of group exponentiation I can take k inside and keep c outside and f_i^k as per the definition of order of f_i will give me the identity element 1 and identity element 1 raised to power c will give me the identity element itself. That means, I have shown that f_1 is a root of x^{n-1}.

I have shown that f_2 is also a root of the polynomial x^{n-1} and f_n is also a root of the polynomial x^{n-1}. That means, I have shown you n roots so, that shows that this fact is true. Now, coming back to this claim, I want to show that among the elements f_1 to f_n there is at least 1 element whose order is n. I will show that if the order of none of the elements f_1 to f_n is n, then I will show that this polynomial x^{n-1} do not have n number of roots. But that will contradict fact number 1 because fact number 1 has been proved, I have established fact number 1. To prove this claim, my strategy will be to show that if there exists no element in the collection F* whose order is n that means the order of f_1 is strictly less than n order of f_2 is strictly less than n and like that order of f_n is also strictly less than n.

Then I will show that this polynomial does not have n number of roots, which will contradict my fact 1 and that will show that indeed this claim is correct that is the proof strategy. But as

I said to prove this implication, so, now, the proof boils down to proving this implication assuming that the statement in the claim is incorrect. To prove this implication, I will take help of several lemmas several related properties.

(Refer Slide Time: 09:08)



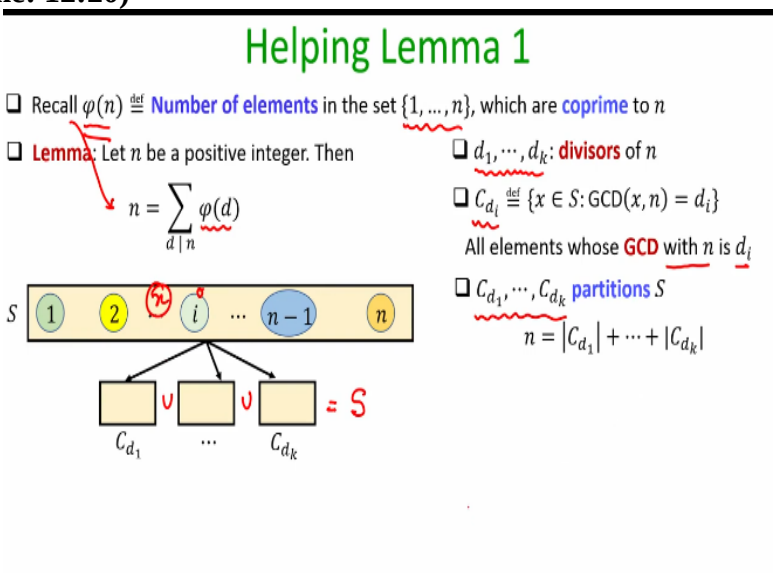
So, let us prove those independent related properties. So, this is helping lemma number 1. So, here I want to prove some property regarding the Euler totient function denoted by φ. So, remember, recall that φ(n) is basically the cardinality of the subset {1, ... , n}, where the elements are co-prime to n. Basically you want to focus on the number of elements in the range 1 to n which are co-prime to n, the number of such elements is denoted by φ(n).

Now we can prove a very nice property in regard for this Euler totient function. The property here is that if you take various divisors here, so, this notation d | n that means d divides n. So, the property here is that if you take various divisors of n, call them as d_1, d_2, d_k and so on and then take the summation of φ of those divisors that will give you the number n. Let us prove this. So, let S be my collection 1 to n and imagine that d_1, d_2, d_k they are the distinct divisors of n.

Now, I am defining a collection C_{di} is basically all those elements from the set S whose GCD with n is d_i. So, what basically I am trying to do here is the following: if I take any number x from the set S and try to find the GCD of that number x along with n, then the GCD has to be one of these divisors of n, because the GCD has to be first of all a divisor of n and the only divisors of n are d_1 or d_2 or d_k. So, that means if I take the GCD of any x here from the set S and number n, it has to be either d_1 or d_2 or d_k.

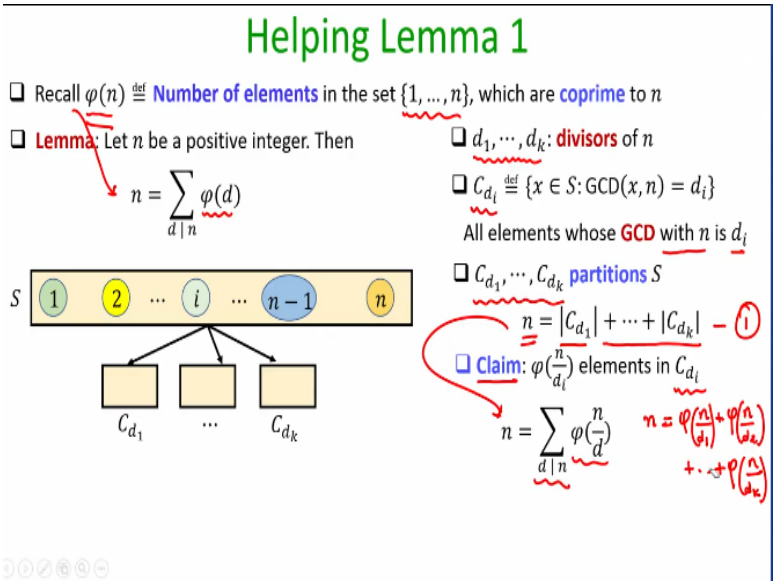
So, I am basically trying to bucket or put all various elements of the set S according to the GCDs that they have with the element n. And the various buckets are C_{d1}, C_{d2} and C_{dk}. Now, as per the definition of this set C_{di}, it is easy to see that this collection is actually a partition of S. It is easy to see that the intersection of these sets is actually empty, because you cannot have a number x whose GCD with n is both d_i as well as d_j. So that trivially shows that the intersection of these collections C_{d1}, C_{d2} and C_{dk} is empty.

(Refer Slide Time: 12:20)



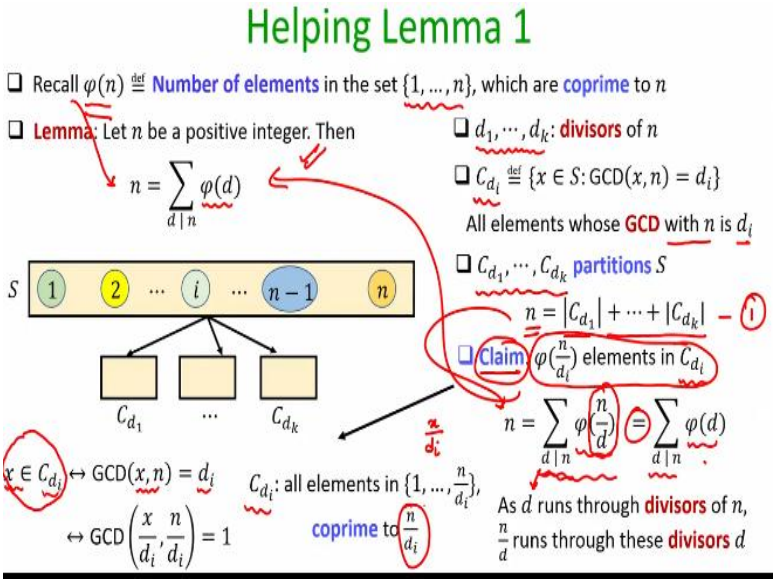
And it is also easy to see that if I take the union of various collections here that will give me the entire set S, because you take any element x, either it will go to the bucket C_{d1} or it will go to the bucket C_{d2} or it will go to the bucket C_{dk}, because if you take the GCD of x with n, it has to be either d_1 or d_2 or d_k a very simple fact here. That means I can say that the summation of the cardinality of these individual buckets is nothing but the cardinality of your set S and the cardinality of your set S is n.

(Refer Slide Time: 12:59)



Now, comes a very crucial claim, my claim here is that the cardinality of the bucket C_{di} is same as the value of the Euler totient function for input $\frac{n}{d_i}$. And remember $\frac{n}{d_i}$ is an integer value because n is divisible by d_i and d_i is a distinct divisor of n. Now, assuming for the moment this claim is true, then, if I apply this claim on this equation $n = |C_{d1}| + ... + |C_{dk}|$, so, call this equation as equation number 1 if I apply this claim on equation number 1, I basically get that n is same as the summation of the Euler totient function for $\frac{n}{d_1}$, the Euler totient function for $\frac{n}{d_2}$ and like that the Euler totient function for $\frac{n}{d_k}$. That is what I have written here your n is summation of various divisors of n and then you sum over the Euler totient function for various $\frac{n}{d_i}$. But now, if you see closely here, if you divide n by a divisor of n, you will obtain a divisor of n itself because d_1, d_2, d_k are the different divisors of n. So, if you divide n by one of the divisors you will get another divisor.

(Refer Slide Time: 14:40)



So, what I can say is I can rewrite this equation and apply the logic that since d here runs through the various divisors of n, this $\frac{n}{d}$ will run through those divisors itself. That means whatever effect I can obtain here the same effect I will obtain if I run through the divisors of n in this summation and instead of taking the summation over $\varphi(\frac{n}{d_i})$, I simply take the summation over φ of the various divisors itself.

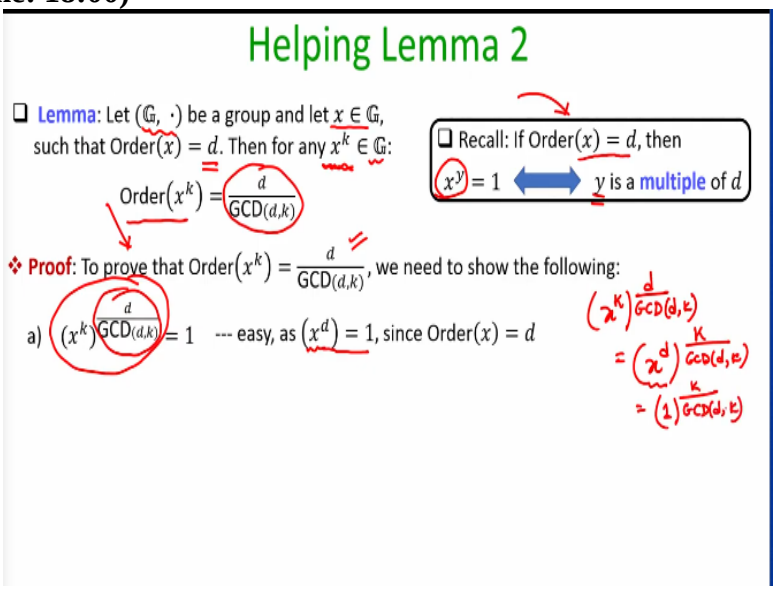
So, it is a very simple fact I am not going to demonstrate; you can easily verify that. The proof for this is that since, d_i is one of the divisors of n and if I divide n by one of those divisors, I will again obtain a divisor in the list d_1 to d_k itself. And that shows the proof of my lemma, but now I have not yet proved this claim. So I have used this claim and then proved my lemma now, the question boils down to how exactly we prove this claim.

So, my goal is now, to prove that there are indeed these many number of elements in the ith bucket, so for that let us try to analyse the property of each of the elements in the ith bucket. So, an element x will be present in the bucket C_{di}, if and only if the GCD(x, n) = d_i that is the definition of the ith bucket. But, if the GCD(x, n) = d_i, then that is possible if and only if the GCD($\frac{x}{d_i}$, $\frac{n}{d_i}$) = 1, very simple.

Because if the GCD($\frac{x}{d_i}$, $\frac{n}{d_i}$) $\neq 1$ and now at the first place the GCD(x, n) was d_i, that means, I can say that only those elements x will be present in the bucket C_{di} such that for those x the GCD($\frac{x}{d_i}$, $\frac{n}{d_i}$) = 1, that means, I can say that ith bucket consists of all the elements in my

collection 1 to $\frac{n}{d_i}$ which are co-prime to $\frac{n}{d_i}$ because any number in the collection 1 to $\frac{n}{d_i}$ which is co-prime to $\frac{n}{d_i}$, say, call that number as $\frac{x}{d_i}$. You multiply that number with d_i that will give you actually a number x which is having a GCD d_i with the element n. And how many elements I have I can have in the collection 1 to $\frac{n}{d_i}$ which can be co-prime to $\frac{n}{d_i}$? As per my definition of the φ function it will be φ ($\frac{n}{d_i}$) and that shows my claim is correct. So, I have proved my helping lemma number 1.

(Refer Slide Time: 18:00)



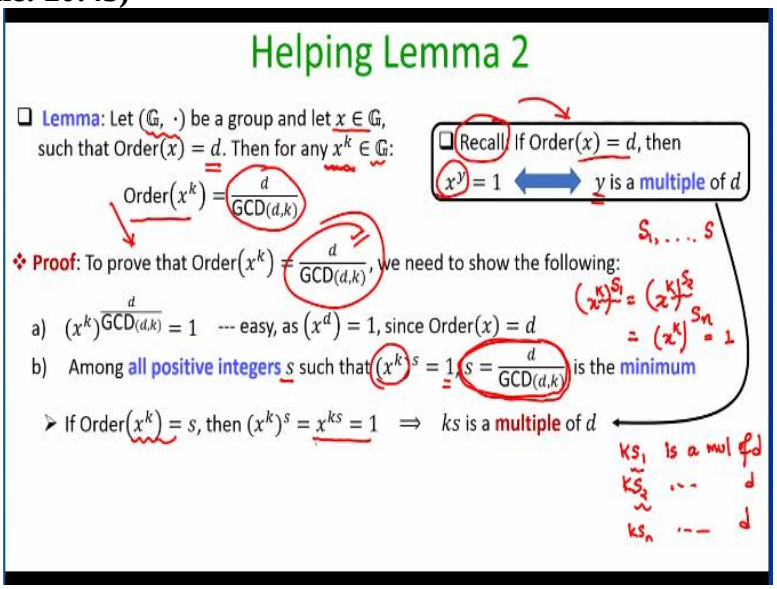
Helping lemma 2 is the following: imagine I take a multiplicative group and imagine there is an element from the group G whose order is d, so, my element is x whose order is d. Then my claim is that for the same element x, if you consider the element x^k and remember x^k as per the rules of group exponentiation is obtained by multiplying the x to itself k number of times, which will be an element of the group itself because my group; since G is a group it satisfies the closure property with respect to the dot operation.

So, the element x^k is actually an element from the group itself. Now, my claim here is that since x^k is an element of the group and it will have some order. Its order will be $\frac{d}{GCD(d,k)}$. So, to prove this statement, I will take the help of some property from the abstract group theory which we had discussed earlier. The property that I am going to use here is that if the element x has order d, and then if you find that x^y is giving you the identity element then that is possible if and only if the exponent y is a multiple of d. So, you can recall the proof of this fact from one of our earlier lecture. Now, my goal is to show that the order of x^k is this value and for that we have to prove two things. The definition of order is, you have to prove that if

you indeed compute this power of the element x^k, you will get the identity element and that is trivial to prove.

Because since the order of x is d, that means x^d is the identity element, then I can say that the element x^k raised to this power will give you the identity element because, if I take x^k raised to power $\frac{d}{GCD(d,k)}$, this is same as x^d whole raised to the power $\frac{k}{GCD(d,k)}$ and x^d is the identity element. Identity element raised to power anything will give me the identity element, this is trivial.

(Refer Slide Time: 20:43)

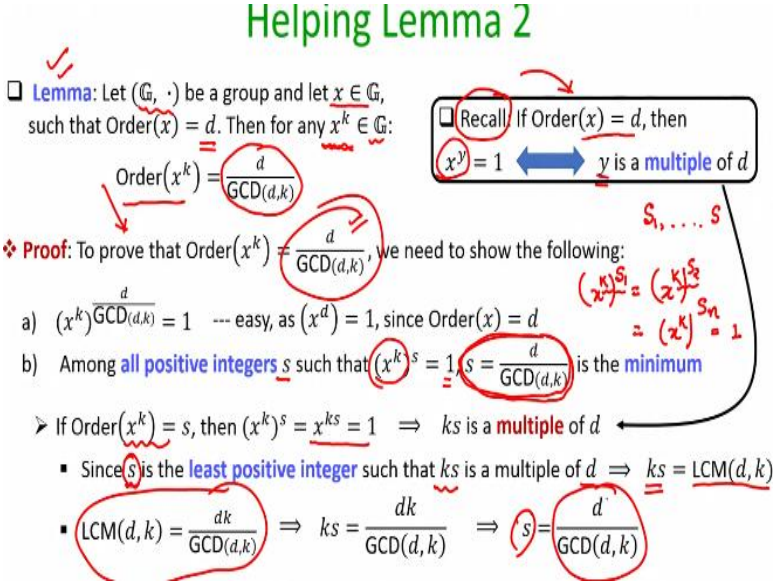


The second thing that we have to prove to show that indeed the order of element x^k is this is the following: I have to show that among all possible different positive powers of x^k such that the s^{th} power or the corresponding power gives you the identity element. The power where s is actually $\frac{d}{GCD(d,k)}$ is the minimum, what basically I am saying is that it is not the case that x^k raised to the power just single s gives you the identity element, there can be multiple exponents s. You can have an exponent s_1 which gives you the identity element, you can have another exponent s_2 which also gives you the identity element and like that, you can have another exponent s_n which also gives you the identity element. So, what I am basically trying to argue here is: in order to show that the order of x^k is this value, you have to show that among the various powers s_1 to s_n the power where the value of the power is $\frac{d}{GCD(d,k)}$ is the minimum one, so, the proof here is as follows.

Since the order of x^k is s, assuming that s indeed is the order of x^k, I know that x^{ks} is 1. And if x^{ks} is 1, I can trigger this result regarding the order of x and I can argue that k times s is a multiple of d. In the same way, k times s_1 is also a multiple of d, k times s_2 is also a multiple of d, k times s_n is also a multiple of d. So, what basically I am arguing here is that if x^k and whole raised to power s_1 is giving you 1, that means k times s_1 is a multiple of d, k times s_2 is a multiple of d and like that k times s_n is also a multiple of d.

Now, I have to focus on the smallest s_i such that this smallest k times s_i which is a multiple of d satisfies the condition that x^{ksi} is giving you the identity element 1.

(Refer Slide Time: 23:34)

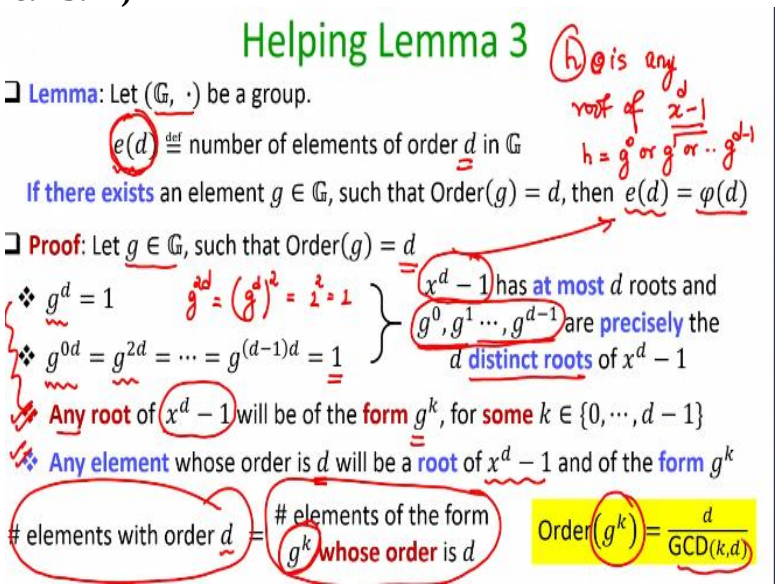


So, what I can say here is the following: if s is the smallest index or the smallest power among these various powers s_1 to s_n satisfying the condition that x^{ks} is 1, then the property of s is that this is the least positive integer of the form k times s which is a multiple of d. That means, I can say that another property of the order s is that: it is such that k times s is the least common multiple of both d and k, of course, k times s is a multiple of k. And k times s will be also a multiple of d, but since s is the order of element x^k that means it is the smallest positive integer such that k times s constitutes LCM(d, k). Now, I can trigger or use the following relationship regarding the least common multiple and the GCD. If I take the LCM(d, k) that will be same as the product of the two numbers divided by their GCD.

And then I can rearrange the terms. Since the LCM(d, k) is k times s. I can substitute LHS by k times s and then I get the conclusion that the smallest positive integer s such that x^{ks} is

the identity element is actually this index ($\frac{d}{GCD(d,k)}$) and that shows the helping Lemma number 2 is also correct.

(Refer Slide Time: 25:22)



And my third helping lemma is the following: the lemma says that if you have a multiplicative group and if you focus on e(d) : all the elements of the group whose order is d; for a given d; then the cardinality of e(d) will be φ(d), if the set e(d) is non empty. Of course, your set e(d) could be empty itself that means there might be no element in the group whose order is d. The lemma says that if your set e(d) is non empty, that means, if there exists at least 1 element in the group whose order is d then actually there are φ(d) of such number of elements.

So, the proof will be as follows: we will take the help of helping lemma number 2 which we have just proved. So, imagine g is an element of the group whose order is indeed d. That means, your set e(d) is not empty and my goal is to show this property regarding the cardinality of the set e(d). Since the order of g is d that means, I can say that element g^d will give you the identity element.

And now, if you see closely here, each of these powers of the element g also will give you the identity element. Say for instance, g^{2d}. g^{2d} can be rewritten as g^d raised to power 2, g^d is 1. So, it will give 1^2 and 1^2 is 1. That means, if I take this polynomial x^{d-1} over the group G, I have shown here that the elements g^0, g^1, g^{d-1} are the distinct d roots of this polynomial x^{d-1}.

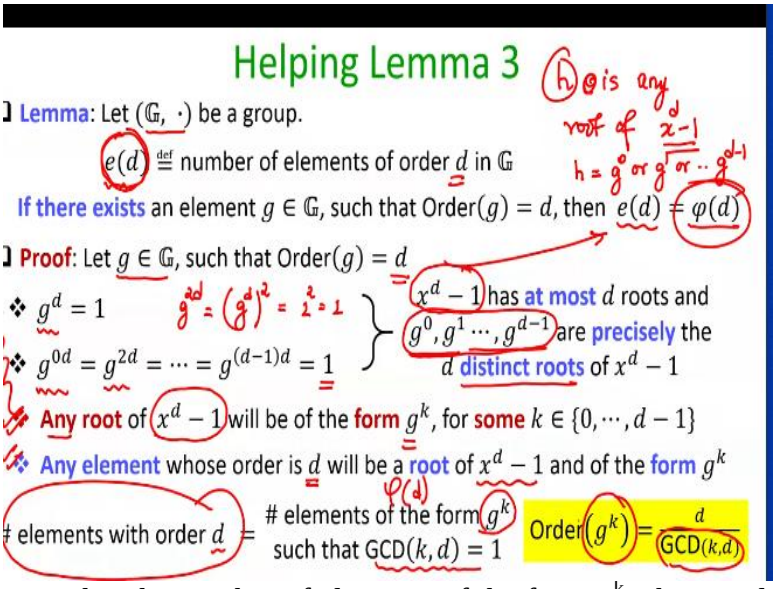
And that is the maximum number of roots that I can have for this polynomial x^{d-1} because this polynomial x^{d-1} is of degree d. So, it can have at most d roots, but I have shown you actually d distinct elements from the group which constitutes the roots of this polynomial. That means, I can say that any root, you take any root of this polynomial, I can relate that root to the element g. What I am saying is that if h is any root of x^{d-1}, then I can say that h is either g^0 or h is g^1 or like that h is g^{d-1}, because I have shown that only roots which are possible for this polynomial are g^0, g^1, g^{d-1}. That means, one of these powers of g will give you the element h where h is some root of the polynomial x^{d-1}. That is a relationship between any root of this polynomial and element g that I have established. And what I also know is that you take any element whose order is d apart from g. So, you take any element say r such that order of r is also d. Then whatever argument I have used here I end up showing that element r also will be the root of this polynomial. Because if g has order d then g constitutes a root of the polynomial x^{d-1}. In the same way if r is an element different from g and its order is d as well, then r is also going to satisfy the polynomial x^{d-1} and so on.

But, I already argued here that you take any root of the polynomial x^{d-1}, it is related to the element g namely, it has to be of the form either g^0 or g^1 or g^2 or some g^k. So, tying these 2 properties together, this property and this property, I can come to the following conclusion, if your goal is to find out various elements whose order is d, then it is equivalent to finding various elements of the form g^k whose order is d.

Because any element whose order is d will be a root of this polynomial and if it is a root of this polynomial x^{d-1} it will be of the form g^k. So, my goal was to find out the number of elements whose order is d. I have reduced that problem to another problem namely finding the number of elements of the form g^k whose order is d, but my helping lemma2 says is that the order of the element g^k will be $\frac{d}{GCD(d,k)}$.

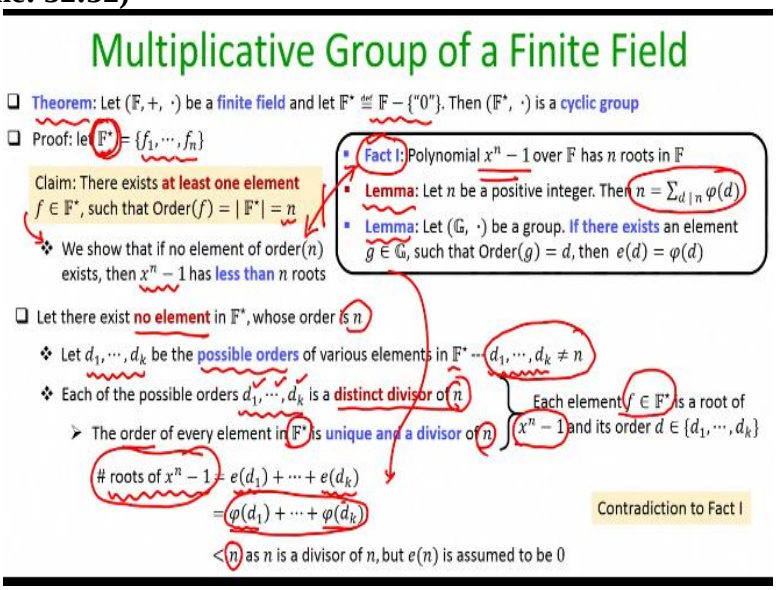
So, when can it be possible that the order of g^k is precisely d? If your denominator becomes 1 namely the GCD(k, d) becomes 1. Because if the GCD(k, d) becomes 1 then I get the order of g^k is d divided by 1 which will be 1.

(Refer Slide Time: 31:51)



That means, I can say that the number of elements of the form g^k whose order is d is equal to the number of elements of the form g^k such that the GCD(k,d) = 1, and how many such k can be there whose GCD with d will be 1. There will be precisely φ(d) number of such k values and that shows that the number of elements in my collection e(d) will be φ(d).

(Refer Slide Time: 32:32)



So, coming back now to the proof of the main theorem, which I wanted to prove. So just to recall I wanted to prove that if I focus on the nonzero elements of the field it constitutes a cyclic group. Basically, I have to show, I have to argue about the existence of a generator. I had already proved this fact and these are my 2 helping lemmas which we had proved. The goal was to show that among the n elements in your collection F* at least 1 element has order n. The proof will be by contradiction.

Namely, we will show that if there exists no element in F* whose order is n then this polynomial x^{n-1} has less than n roots and that will go against this fact number 1. So, let us prove this claim now. Assume that none of the elements from F* has order n. So, let the various orders which are possible, namely, I have listed down the orders of various elements from your set F* and let those orders be d_1 to d_k.

So, you have n elements, it is not the case that all of them have distinct orders. It might be possible that order of f_1 is same as order of f_2, order of f_3 and so on. So, it is not necessary that since you have n elements, you have n distinct orders and few of the orders may be repeated. So that is why let k be the possible orders for various elements in F*. And since I am assuming that there is no element in F* whose order is n, that means none of these orders d_1 to d_k is n.

Now I also know that each of these possible orders d_1 to d_k is a distinct divisor of n. They are distinct because they are the various possible distinct orders and why it is a divisor of n because I know that order of any element from F* which actually is a group divides the order of F*, the order of F* is n. So, that is why order of f_1 will be a divisor of n, order of f_2 will be a divisor of n, order of f_n will be a divisor of n.

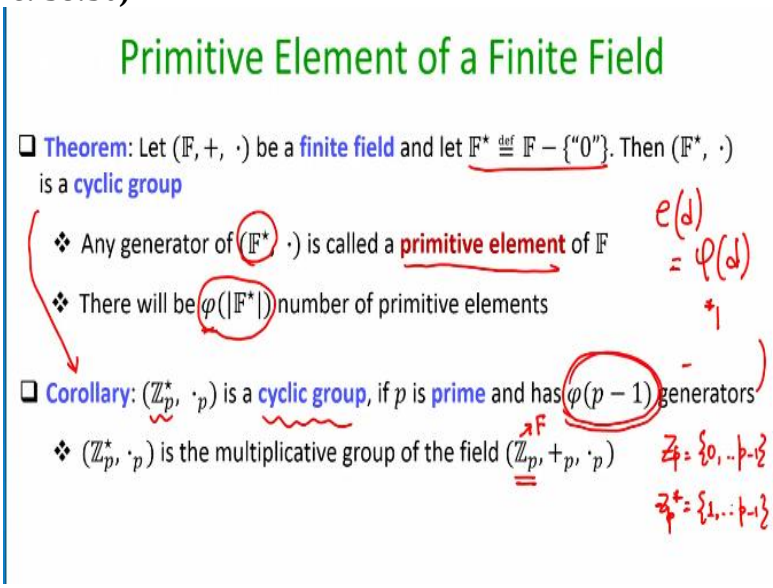
Now, when I proved the fact number 1, I also argued, I also showed there that you take any element from F* f_1, f_2, f_n each of them is a root of this polynomial. And as per our assumption, that order of F will be either d_1 or d_2 or d_k. So, by tying these two facts together, what I can say about the number of possible roots for this polynomial? The number of possible roots will be, namely, the number of elements with order d_1, the number of elements with order d_2 and the number of elements with order d_k. If I sum the number of elements with these orders that will basically give me the number of roots for this polynomial x^{n-1}. Because among the elements from F*, the orders that are possible are either d_1, d_2, or d_k. And each element from F* is actually a root of x^{n-1}. So, that is why I get this equation (# of roots of $x^n - 1 = e(d_1) + ... + e(d_k)$). Now, I will use this helping lemma here and I can say that the number of elements in F* whose order is d_1 is nothing but $\varphi(d_1)$.

In the same way the number of elements from F* with order d_k is nothing but $\varphi(d_k)$ and so on. And what can I say about the summation in my RHS? The summation in the RHS is

strictly less than n: why it is strictly less than n? Because even though d_1, d_2, d_k they are distinct divisors of n, as per my assumption, none of them is actually n.

That means, neither d_1 is n, nor d_2 is n and so on. And as per the helping lemma 1, only when I sum over φ of various distinct divisors of n, I will get the value n. But since none of these divisors d_1 to d_k is n that means I am missing at least one distinct divisor of n. And that is why I can say that if I take the summation of these quantities $\varphi(d_1)$, $\varphi(d_2)$, $\varphi(d_k)$, I would not be getting the full n. If there would have been a divisor, if that means if I would have included φ(n) here as well, then I can say that the summation of all these things is n, but since φ(n) is missing here because as per my assumption there is no number, no element, from F* with order n, I can say that my RHS is actually strictly less than n. My RHS is actually the number of roots of this polynomial. So, this goes against the fact 1 because I have separately shown already that indeed there are n number of elements from F which constitutes the root of this polynomial. In fact, all the elements of F* satisfy this polynomial and that is possible only if at least 1 of the elements from F* has order n. So that proves the theorem.

(Refer Slide Time: 38:50)



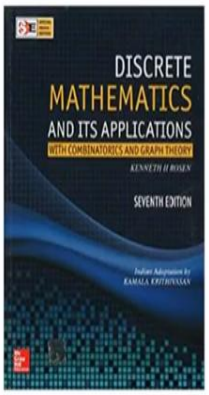
So now, let us apply this theorem here. So we have proved that you take any finite field and if you focus on the nonzero elements, we have shown it constitutes a cyclic group. That means, the collection F* along with the dot operation will have a generator and the generator is also called as the primitive element of your entire field. And how many such primitive elements will be there? You will have φ(|F*|) number of such primitive elements.

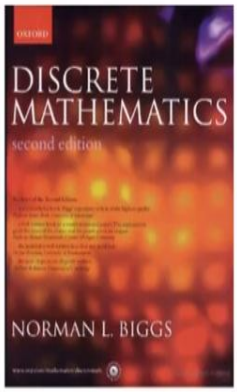
Because as per our helping lemma there are φ(d) number of elements with order d. So, we basically want to find out how many elements are there with order same as the order of your F*. So, it will be same as φ(|F*|). And now if I apply this theorem for the special case of the field, $\mathbb{Z}_p$. So, your $\mathbb{Z}_p$ will have all the elements from 0 to p - 1 and if I say $\mathbb{Z}_p$*, then it will have p - 1 elements. All the elements except 0 are present here.

Since $\mathbb{Z}_p$ constitutes a field, if I focus on the nonzero elements, I get $\mathbb{Z}_p$* and if I apply this theorem, I get the conclusion that your $\mathbb{Z}_p$* is a cyclic group and it will have these many number of generators (φ(p – 1)). And this is a very crucial property which if you recall we utilized to during our discussion on Diffie-Hellman key exchange protocol and Elgamal encryption scheme; there we performed operations over $\mathbb{Z}_p$* and there I assumed that it is a cyclic group with some generator.

There you might be wondering what is a guarantee that indeed $\mathbb{Z}_p$* is a cyclic group. Now, we have proved that indeed $\mathbb{Z}_p$* is a cyclic group and it will have many generators it will have φ(p – 1) number of generators.

References for Today's Lecture





(Refer Slide Time: 41:00)

So, with that I conclude today's lecture. Just to summarize today, we discussed about the multiplicative group of a finite field and we proved that it is a cyclic group. The generators of that cyclic group are also called as the primitive elements of your finite group.