

A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 23
Euler φ -function - I

Welcome back, we will be talking about Fermat's little theorem. So, the Fermat's little theorem says that if you have a p to be a prime and you take any nonzero element in \mathbb{Z}_p , then a power p minus 1 is congruent to 1 modulo p . Now, I also told you that there are some knotty numbers which satisfy Fermat's little theorem, but there we have to be slightly careful.

What happens is that if you have a number a in \mathbb{Z}_n , which is co-prime to n , only then we can expect a power p minus 1 to be 1 modulo n because if the GCD of a and n is bigger than 1, then ofcourse all the powers of a will have GCD with n bigger than 1 and therefore all these powers cannot be equal to 1.

So, indeed Fermat's little theorem can be used to find whether a given number is prime or not. However, there are some numbers n which have the property that there is some a less than n , which has the possibility that a power n minus 1 is 1 modulo n . So, if you were to start with the given n , you were to start with choosing a random number a in \mathbb{Z}_n and then checking a power n minus 1 it may happen that you get it to be 1 modulo n but n need not be prime.

I will let you find more information about this by working out some examples. For the moment we will go ahead with something else. What we now want to do is to observe that there are elements in \mathbb{Z}_n which behave in a nicer way. So \mathbb{Z}_p has very nice arithmetic because whenever you take any 2 elements in \mathbb{Z}_p which are not 0, their product gave you a non-zero number, this is not true in general for \mathbb{Z}_n .

Again, for instance, if we are taking n equal to 8, there are these 2 numbers 2 and 4, these are not 0 modulo 8, but their product is 0 modulo 8. So, these are the elements, the 0 divisors in \mathbb{Z}_n , which create problem for the arithmetic in \mathbb{Z}_n . So, we would like to take these elements out or in other words, we want to find elements which have the property that they are not 0 divisors.

What does it mean to say that something is not a 0 divisor? It means that when I take such an element a in \mathbb{Z}_n and I multiply by various b s, then I do not get 0, I would always get non-zero elements. When can such a thing happen? So for instance, if your element a happens to

be equal to 1, then 1 into any number will give you that number, 1 into a always gives you a, it will never give you 0 unless a itself is equal to 0.

So, when you have such a number, one more just an example, we would like to find elements such that when you multiply to them by any non-zero number you should get a non-zero number modulo n, you should not get something which is 0. But after all you have only finitely many elements and when you are going to look at it modulo n, you have the property that $a \cdot i \equiv a \cdot j \pmod{n}$ implies $i \equiv j \pmod{n}$.

And if your a has the property that $a \cdot i \equiv a \cdot j \pmod{n}$ implies $i \equiv j \pmod{n}$ that will tell you that whenever you have $a \cdot i \equiv a \cdot j \pmod{n}$, you will have that $i \equiv j \pmod{n}$. So, the elements which have the property that they are not 0 divisors, these are also the elements which can be canceled and we want to find the set of these elements.

(Refer Slide Time 04:45)

We are interested in finding elements of \mathbb{Z}_n which are invertible in \mathbb{Z}_n .

These are the elements $a \pmod{n}$ such that

$$a x \equiv 1 \pmod{n}$$

has a solution.

Equivalently, we are searching for a with $(a, n) = 1$.

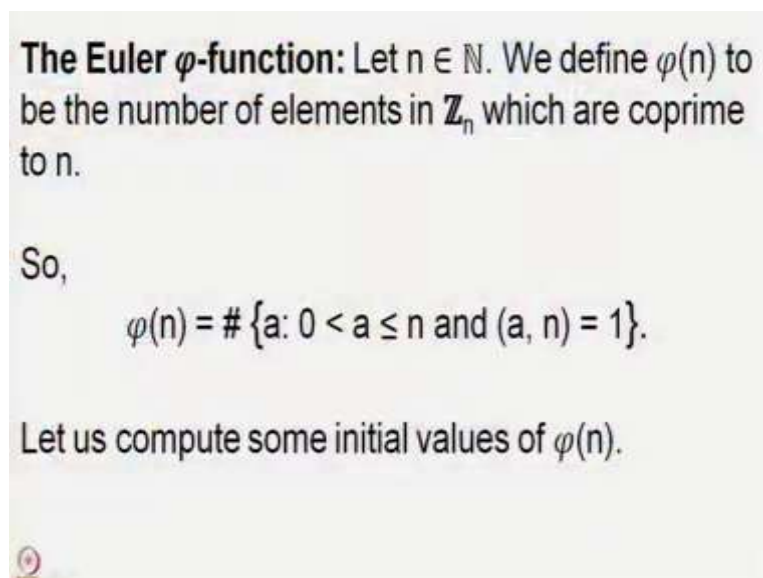
So, in other words, these are elements which are invertible in \mathbb{Z}_n so, that is there is some another element b in \mathbb{Z}_n with the property that $a \cdot b$ will give you 1, so what we are looking for are the elements a , modulo n such that $a x \equiv 1 \pmod{n}$ has a solution, we should have a solution for the linear congruence $a x \equiv 1 \pmod{n}$.

Now, linear congruence is something that we are trained so well in, that even if I wake you up in your sleep, you should be able to give me the condition for the existence of solution here, you should be able to tell me right away that the GCD of a and n divides 1.

Now GCD of a and n divides 1 in natural numbers will tell you that the GCD be better equal to 1. So, these are all the elements a with the property that the GCD of a and n is 1. So, starting from something which had something to do with the multiplication in \mathbb{Z}_n asking For elements which are inevitable in \mathbb{Z}_n , we have now come up with a number theoretic concept that the GCD of these numbers and n should be equal to 1.

If you observe that whenever n is a prime p , this condition a, n equal to 1 holds for all numbers less than p except of course 0. So, these are the numbers that we are looking for, these are the numbers which are all the elements in \mathbb{Z}_p , all the non-zero elements in \mathbb{Z}_p , these are the nice elements in \mathbb{Z}_n which we are looking for.

(Refer Slide Time 06:50)



The Euler φ -function: Let $n \in \mathbb{N}$. We define $\varphi(n)$ to be the number of elements in \mathbb{Z}_n which are coprime to n .

So,

$$\varphi(n) = \# \{a: 0 < a \leq n \text{ and } (a, n) = 1\}.$$

Let us compute some initial values of $\varphi(n)$.

As mathematicians are trained to do, perhaps what we then do is that we define a function. You may think that it would be easier to compute this for particular n s, but mathematicians will tell you by experience and rightly so, that it is good to have this function defined for all n and then study the property of this as a function from natural numbers to natural numbers.

So, we define this function $\varphi(n)$, this is a function, and what does it do? It computes the number of elements in \mathbb{Z}_n . Remember this is \mathbb{Z} by n \mathbb{Z} which are co-prime to n that means these elements are the ones which are not the 0 divisors when you are looking at them in \mathbb{Z}_n . So, $\varphi(n)$ which is the function that we have just now defined is the cardinality of all the numbers from 0 to n with the property that the GCD of these numbers with n is equal to 1.

It may look like a very daunting thing, we are going to study all properties of this function which is now defined for all n , but that is the beauty in mathematics that when you generalize

something then studying it becomes much simpler. So, for the moment, let us try to compute some values of $\phi(n)$.

(Refer Slide Time 8:27)

Examples:

1. $\phi(1) = 1,$
2. $\phi(2) = 1,$
3. $\phi(3) = 2,$
4. $\phi(4) = 2,$ $\{1, \cancel{2}, \cancel{3}, 4\}$ $(2,4)=2 > 1,$
 $(4,4)=4 > 1.$

Ofcourse, $\phi(1)$ is 1 because there is the element 1 which is less than or equal to, and you have so here the number of elements that you are looking for is simply the singleton 1. This is the element which goes from 0 to n and has the GCD 1 with n , n itself being equal to 1. Second is $\phi(2)$. so we are going to look at this set \mathbb{Z}_2 or you may say, we are looking at the set 1, 2, this is the set \mathbb{Z}_2 and you remove the elements which are not co prime 2, 2.

So again here we are left with only one element which is singleton 1. If you go one step further $\phi(3)$, this happens to be 2. Let us write all the elements from 1 to n , and now we remove the element which is not co-prime to 3. 1 and 2 happened to be co-prime to 3, so here the value of the function ϕ at the number 3 is equal to 2.


$\phi(4)$, once again, here we write all the elements of \mathbb{Z}_4 , this will have to be removed and 2 will also have to be removed because 2 is also not co-prime to 4, the GCD of 2 and 4 is 2, which is bigger than 1, as well as the GCD of 4 and 4 is 4 which is also bigger than 1. So these are the two elements which we need to remove and so $\phi(4)$ is indeed equal to 2. You may now think that we had 1, 1, and then 2, 2.

And if you ask anybody to complete the sequence ahead or compute the sequence ahead, the most natural answer would be 3.

(Refer Slide Time: 10:46)

Examples:

1. $\varphi(1) = 1,$
2. $\varphi(2) = 1,$
3. $\varphi(3) = 2,$
4. $\varphi(4) = 2,$
5. $\varphi(5) = 4, \{1, 2, 3, 4\}$




But if you want to compute phi of 5, the Euler phi function of the number 5, you will get it to be 4. And the reason being that all 1, 2, 3, 4 are co-prime to Phi. 5 is the thing that you will have to remove, so you are left with 4 elements, so phi of 5 is 4.

(Refer Slide Time: 11:16)

Examples:

1. $\varphi(1) = 1,$
2. $\varphi(2) = 1,$
3. $\varphi(3) = 2,$
4. $\varphi(4) = 2,$
5. $\varphi(5) = 4,$
6. $\varphi(6) = 2, \{1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}\} = \{1, 5\}$

$(4, 6) = (2, 6) = 2 > 1,$
 $(3, 6) = 3 > 1.$



And now brace yourself, phi of 6 is equal to 2, it is a smaller number, then phi of 5. The sequence is not quite an increasing sequence so let us write all the numbers up to 6 and let us see where we are getting the GCD to be not equal to 1, GCD of 6 with itself is 6.

So that has to be removed, 4 has to be removed because the GCD of 4 and 6 is equal to the GCD of 2 and 6 which is to 2, 2 also needs to be removed. 3 also needs to be removed

because 3 and 6, the GCD is 3, all the GCD is are bigger than 1. So the only set that is left is the set 1, 5 therefore phi of 6 is equal to 2.

(Refer Slide Time: 12:15)

Examples:

1. $\varphi(1) = 1,$
2. $\varphi(2) = 1,$
3. $\varphi(3) = 2,$
4. $\varphi(4) = 2,$
5. $\varphi(5) = 4,$
6. $\varphi(6) = 2,$
7. $\varphi(7) = 6,$

$\varphi(p) = p - 1.$

Now from the example of phi 5, you should be ready for the answer of phi 7, and that answer is indeed equal to 6. In fact, you should be able to generalize this by saying that whenever we are looking at a prime p , phi of p is equal to p minus 1. In fact, we have also seen this that in \mathbb{Z}_p all the non-zero elements are invertible, you can invert all the non-zero elements, and therefore, phi of p is p minus 1.

(Refer Slide Time: 12:46)

Examples:

1. $\varphi(1) = 1,$
2. $\varphi(2) = 1,$
3. $\varphi(3) = 2,$
4. $\varphi(4) = 2,$
5. $\varphi(5) = 4,$
6. $\varphi(6) = 2,$
7. $\varphi(7) = 6,$
8. $\varphi(8) = 4.$

$\varphi(p) = p - 1$

$\{1, 3, 5, 7\}, (4, 8) = 4 > 1,$
 $(2, 8) = (6, 8) = 2 > 1, (8, 8) > 1.$

Let us check 1 more example, phi of 8 and this happens to be 4. So, this is because when you write all the elements modulo 8, we can write only the odd elements, once you have even element that will have a non-trivial GCD with 8, so the GCD of 2, 8, the GCD of 6, 8 are equal to 2 which are bigger than 1, the GCD of 4, 8 is 4, which is bigger than 1.

And ofcourse, the GCD of 8 with itself is 8, which is bigger than 1. So here we are left with only 4 numbers from 1 to 8, which are co-prime to 8. This is how the values of all these elements can be computed. And as we have observed when you have phi of p to be p minus 1, we can actually write down the values for most of these numbers.

For instance, the value of 2, phi of 2 is 2 minus 1, phi of 3 is 3 minus 1, phi of 5 is 5 minus 1 and phi of 7 is 7 minus 1 this could ofcourse be written without even having to worry about it. These other quantities phi of 4, and phi of 8, these are prime powers. And then this is something which is still something complicated, which is that it is a product of two different primes.

So to be able to compute the values of this Euler phi function, what we are going to do is to define, is to have a result which allows you to compute the phi values for a prime power, which will explain all the terms here in this table except the term phi 6, the Euler phi function at 6 which is equal to 2, so that is a very nice result. The result simply says that whenever p is a prime and you want to compute the Euler phi function on p power e for any e.

(Refer Slide Time 15:01)

Lemma: If p is a prime then

$$\varphi(p^e) = p^e - p^{e-1}.$$

This explains all the values on the previous slide, except the value $\varphi(6)$.

$$\varphi(4) = \varphi(2^2) = 2^2 - 2^1 = 4 - 2 = 2.$$
$$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4.$$
$$\varphi(9) = \varphi(3^2) = 3^2 - 3 = 6. \quad \{1, 2, 4, 5, 7, 8\}$$

Here there is no restriction on e , any power e , then φ of p power e is simply p power e minus p power e minus 1. So, this explains all the values on the previous slide except the value φ of 6. This is because if I wanted to find φ of 4, which is φ of 2 square, this would be by our previous formula φ of 2 square minus 2 power 1 which is 4 minus 2 and therefore, it is equal to 2.

Similarly, φ of 8 which is φ 2 cube is 2 cube minus 2 square which gives me that it should be 4. This should tell you that if you wanted to compute the net φ value which we did not, but if you wanted to compute this, this would be φ of 3 square, which will be 3 square minus 3, and therefore, this will be equal to 6.

Indeed, if you were to look at the elements, then you will have to remove 3, you will remove 6, and these are the elements modulo 9, which are all co prime to 9, so these are 6 in number. This is how the φ values can be computed for all prime powers.

(Refer Slide Time: 16:40)

Lemma: If p is a prime then

$$\varphi(p^e) = p^e - p^{e-1}.$$

This explains all the values on the previous slide, except the value $\varphi(6)$.

We will later see a result for computing the general φ values.

Ofcourse, every number is not a prime power, so we will also let us see a result which will allow us to compute general phi values. So, for the moment we go ahead with the proof of this very nice result that whenever we have p to be a prime then $\varphi(p^e) = p^e - p^{e-1}$. And the proof is just the counting proof, we will write.

(Refer Slide Time: 17:15)

Lemma: If p is a prime then

$$\varphi(p^e) = p^e - p^{e-1}.$$

Proof: $(a, p^e) = 1$ if and only if $(a, p) = 1$.

1	1, 2, 3, ..., p	Not coprime to p . $(a, p) \neq 1$ $\Leftrightarrow p a$. rows are p^e/p .
2	$p+1, p+2, p+3, \dots, 2p$	
3	$2p+1, 2p+2, 2p+3, \dots, 3p$	
	\vdots $p^e - p, p^e$	

First of all, we observe that $(a, p^e) = 1$ if and only if $(a, p) = 1$. So if you have a natural number, and it has GCD equal to 1 with respect to a prime power p^e then clearly it is GCD with p has to be 1 because p divides that prime power. If the GCD of A and p is not 1, then it would be bigger than 1 and then it will have to be p because p has no other divisors other than 1 and p .

And if p divides a then p will divide a as well as p^e and therefore, the GCD of a and p^e cannot be 1. So, whenever the GCD of A and p^e is 1, the GCD of a , p has to be 1 and if GCD of a , p is 1, the GCD of a and p^e also has to be 1 because p is the only prime that divides p^e .

So, when we are counting elements modulo p^e , so we will start with 1, 2, 3 and write down all the elements up to p^e . And among these, we will have to find elements which are not co-prime to p^e and remove them. We simply have to find elements which are not co-prime to p and remove them that is how simple it is.

So, we start by writing the elements modulo p^e . So, we have 1, 2, 3 so on up to p , then we start writing the elements in the next row $p+1$, $p+2$, $p+3$ dot, dot, dot and then the next multiple of p will be $2p$. After that we have $2p+1$, $2p+2$, $2p+3$, $3p$ and we can just continue this way.

The last one, before p^e would be where you will have this to be $p^e - p$, and the last one would be the number p^e . At each stage we are adding p , we add p and get $2p$, we add p and get $3p$ so that here we will add p and get the number p^e . And these are the only numbers which are not co-prime to p .

Because to have some a^p not equal to 1, this is equivalent to p dividing the number and we have counted exactly the multiples of p going from 1 to p^e . How many multiples have we found? Let us count this as 1, this is 2, this is 3 and so on. The total number of rows here is p^e upon p , these many rows we have.

(Refer Slide Time 20:53)

Lemma: If p is a prime then
 $\varphi(p^e) = p^e - p^{e-1}$.

Proof (contd.): $\varphi(p^e) = p^e - \underbrace{\#\{1 \leq a \leq p^e : p|a\}}_{\substack{\text{no. of rows in the} \\ \text{last slide} \\ p^{e-1}}}$

$\varphi(p^e) = p^e - p^{e-1}$.

So $\varphi(p^e)$ is p^e minus the number of elements 1 up to p^e with the property that p divides a and this number as we have seen is the number of rows in the previous slide which is nothing but p^e minus 1 and therefore, we get that $\varphi(p^e)$ is equal to p^e minus p^{e-1} , a very simple truth.

So, this is the proof that allows us to compute the φ value for any prime power. Now, to go for a general n what we have is that a general n will be product of prime powers. So, if we had a way to go from product of different prime powers, from prime powers to their product, then we would be able to compute the φ value for all such numbers.

(Refer Slide Time 22:26)

Lemma: If $(a, b) = 1$ then $\varphi(ab) = \varphi(a) \varphi(b)$.

Proof:

- ① Note that $(\alpha, ab) = 1$ if and only if $(\alpha, a) = 1$ and $(\alpha, b) = 1$.
- ② If $\alpha \equiv \beta \pmod{a}$ then $(\alpha, a) = (\beta, a)$
- ③ $\alpha \equiv \beta \pmod{b}$ then $(\alpha, b) = (\beta, b)$

So, here is the next lemma, which says that whenever a, b is 1, then $\varphi a, b$ is the product $\varphi a \varphi b$. So, once you have this lemma, this will tell you that you can compute the φ value for all numbers, you will simply write n as product of distinct prime powers.

For each prime power, we know how to compute the φ value and to find the φ value of the number n , you simply have to take the product of the φ p power e , whenever p power e is the exact divisor of n for the prime p . So, even this proof is not difficult, so one would prove this in the following way.

Note, first of all that some α is co prime with a, b if and only if α is co-prime to a and α is co-prime to b . This is the first major thing that we need to observe. How does one think about proving this? Suppose we have so this is again, I have been telling you that whenever we have, if and only if, it means that if this holds and this holds then we should get this. This is the Meaning of if, $(\alpha, a, b) = 1$ if $(\alpha, a) = 1$ and $(\alpha, b) = 1$.

So, how does 1 prove this? If you have that $(\alpha, a) = 1$ and $(\alpha, b) = 1$ and suppose now that $(\alpha, ab) \neq 1$, so we are assuming the contradictory. We are assuming the contrary, we are assuming that (α, ab) is bigger than 1 but $(\alpha, a) = 1$ and $(\alpha, b) = 1$.

So, take the GCD d of α and ab and take a prime divisor of that, since that number is bigger than 1 it should have a prime factor. If that p is the prime factor, which divides α and also the product ab , then you know what we are going to do. We will take p that has to divide either a or b ; p being a prime when it divides ab , it will have to divide either a or b .

If p divides a then $\gcd(a, b)$ will have a prime factor, the GCD of a, b will have p in it. If p divides b , then the GCD of a, b will have p in it. So, whenever $\gcd(a, b) = 1$, a and b will also have to be equal to 1.

Okay, so, if condition is done, and now to get the only if condition, we go in the reverse way, if you have that $\gcd(a, b)$ or $\gcd(a, b)$ any of these 2 is bigger than 1, then $\gcd(a, b)$ has to be bigger than 1 because once again, let us say $\gcd(a, b)$ is bigger than 1, take a prime p dividing it, that prime will have to divide both a and b because it divides a and it divides b .

So when you have a prime dividing $\gcd(a, b)$, and a, b , the GCD of a, b cannot be 1, it will have to be bigger than 1. Think about this proof, but it is a simple enough proof. So, when you are looking at elements which are co-prime to the product a, b , you have to have those elements to be co-prime to both a and b , this is number 1.

Second property that we observe is the following. That if you have $a \equiv b \pmod{m}$, then the GCD of a, m is equal to the GCD of b, m . And similarly when you have $a \equiv b \pmod{m}$, then the GCD of a, m is equal to the GCD of b, m . So, these are the 2 things which can be seen quite simply and therefore, we will not see the proof of these things.

But we will just assume these both statements, which says that if you have in particular, it will say that if you have some number which is co-prime to a , by adding multiples of a to it, you will still get a number which is co-prime to a , and the same thing will be true for the number b . So, now we want to compute the number of elements which are co-prime to a, b in terms of the numbers which are co-prime to a and the numbers which are co-prime to b .

(Refer Slide Time: 27:50)

Lemma: If $(a, b) = 1$ then $\phi(ab) = \phi(a) \phi(b)$.

Proof (contd.):

The diagram shows a grid of numbers from 1 to ab . The first row contains $1, 2, 3, \dots, i, a$. The second row contains $a+1, a+2, a+3, \dots, i+a, 2a$. The third row contains $2a+1, 2a+2, \dots, i+2a, 3a$. The grid continues down to $a(b-1)$ and ab . A vertical column containing $i, i+a, i+2a, \dots, i+(b-1)a$ is circled. A note above the grid says "(i, a) = 1". A note to the right says "remove numbers which are not coprime to a". A note below the grid says "all these are going to be removed". The set Z_{ab} is indicated.

So, the proof would go again by writing all these elements as multiples of a ; $3a$, and so on. The last thing here would be a , and you are just adding a every time so the last but one thing would be a into b minus 1, this is how we would have all these a terms. These are all a terms, so you are actually looking at z a .

And here we are now going to find elements which are co-prime to a, b . So in this row, we have to remove elements which are not co-prime to a, b . And for that, what we do is that we remove elements which are not co-prime to a . So, here remove numbers which are not co-prime to a .

Suppose that there is an i here, which is not co prime to a , then all these elements in the column of i will have the property that these are going to be i plus a multiple of a . All these elements are i plus a multiple of a and therefore all these will have to be removed. So, all these going to be removed because all of these are not co-prime to a and therefore, they are not co-prime to a, b . So, when we remove a particular number i from here, we are removing a particular column.

(Refer Slide Time: 30:41)

Lemma: If $(a, b) = 1$ then $\varphi(ab) = \varphi(a) \varphi(b)$.

Proof (contd.): Thus, we have kept only $\varphi(a)$ columns of the table. Each column of the table lists all elements of \mathbb{Z}_b modulo b . Hence, to obtain $\varphi(ab)$ we need to remove, from each column the elements which are not coprime to b .

And thus in the table we have kept only $\varphi(a)$ columns of the top the table, only $\varphi(a)$ columns are kept. Further each column of the table lists all elements of \mathbb{Z}_b modulo b . Let us think about this statement for 5 seconds. We are saying that we are only going to look at the columns of the table.

So the columns remember they start with some element which is from 1 to a , and then you keep adding a to those elements, but a is co-prime to b therefore, when you look at mod b , a is an invertible element. Therefore, when you start with any element module any element from 1 to a and then you keep adding a to them, you are going to get all other elements in \mathbb{Z}_b .

First of all you have b elements because there are b rows and so you have say some j , then j plus a , j plus $2a$, all the way up to j plus $3a$, j plus a into b minus 1. And no 2 of these can be equal because j plus αa equal to j plus βa modulo b will tell you that αa is βa modulo b , but a is invertible modulo b being co-prime to b so, it tells you that α is β . So, the b elements that you have obtained they are all distinct modulo B .

So in this table each column if you for instance, look at the column corresponding to 2, you are going to get all b elements modulo b when you reduce them modulo b , and therefore, each column looks like the elements of \mathbb{Z}_b in a different order. And hence to obtain elements which are co-prime to b , so we are looking to obtain elements which are co-prime to a , we need to remove from each column the elements which are not co-prime to b .

We will have to remove the elements which are not co prime to b from each column. Earlier what we had done was that we have removed elements which are not co prime to a, we observe that if there was any element from 1 to a b, which was not co prime to a then modulo a it will correspond to some element from 1 to a with the property that that element is not co prime to a, this is the content of those 2 remarks that we have observed at the beginning of the proof.

And similarly, now from each of the remaining columns, we will have to remove elements which are not co prime to b. so the elements which are left in each column now is equal to phi b. These are the elements which are co-prime to b.

(Refer Slide Time: 35:06)

Lemma: If $(a, b) = 1$ then $\varphi(ab) = \varphi(a) \varphi(b)$.

Proof (contd.): We have $\varphi(a)$ columns and in each column we have only $\varphi(b)$ elements.

Thus, $\varphi(ab) = \varphi(a) \varphi(b)$.

$a=3, b=4,$

1	2	3	4
5	6	7	8
9	10	11	12

$\varphi(4)=2$.

So, to summarize, we have phi a columns and in each column we have only phi b elements, because we have removed all the elements which are not co-prime to b, so we are left with only the elements which are co-prime to b and that number is phi b and thus we get that phi a b is phi a into phi b.

Just to give you an idea of this proof, let me work this proof out in the very special case where we have a equal to 3 and b equal to 4, so we are looking at 12. And then we would look at 1, 2, 3 or let me put 4 next to 3, so that we have some space 5, 6, 7, 8, 9, 10, 11 and 12.

And from these now, for the numbers 1,2, 3, 4 to remove numbers which are not co-prime with 4, we have to remove 2 and 4 and then automatically 6, 10, 8 and 12 get removed. So, we have exactly 2 columns left which is equal to the number phi 4 remember phi 4 is 2. And

now from each of these columns, we will go modulo 3 and we will see which are not co-prime with 3, 9 is not co prime with 3 and here 3 is not co-prime with 3.

So, there are 2 columns which is equal to phi of 4 and in each of these 2 columns, we are exactly going to have only 2 elements, which is phi of 3. So, this is how the general proof works. There is not much that I can say after this, so please think about this proof and if you have any problem in understanding this proof, please write back to me and I will try to respond to all such queries. I hope to see you in the next lecture. Thank you.