

A Basic Course in Number Theory
Professor Shripad Garge
Indian Institute of Technology, Bombay
Department of Mathematics
Lecture 24

Euler φ -function - II


Welcome back, we are studying the Euler phi function, we saw the definition of this function and we saw 2 basic properties. So, the first 1 was that whenever your number is order of a prime, then we know what the value of the Euler phi function should be. And secondly, when you have 2 co prime numbers a and b , then we saw that the Euler phi function of the product $a b$ is the product of the Euler functions.

(Refer Slide Time: 00:53)

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,

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


So, just to recall we have φn for every natural number n and, you know this equality sign here is important only because we should have that φ of 1 be equal to 1 for all others, we will of course not have n here. So, this is our definition of the Euler phi function, φn to be the cardinality of all the numbers from 1 to n , which are relatively prime to n .

(Refer Slide Time: 01:26)

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

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

These two lemmas enable us to compute the $\varphi(n)$ in general.

$$n = p_1^{n_1} \cdots p_k^{n_k}$$
$$\varphi(n) = \varphi(p_1^{n_1}) \cdots \varphi(p_k^{n_k}).$$

And then we saw these 2 results that whenever your number is prime power then the phi function is given by this formula, it is p power e minus p power e minus 1. And the second statement tells you that whenever a and b are co prime then $\varphi(a b)$ is $\varphi(a)$ into $\varphi(b)$. So, these 2 lemmas enable us to compute the Euler phi function in general and the way to go about that would be that you write n as your product of distinct prime powers and after that we observe that we should have this property. This is how one would compute the Euler phi function in general. There is however, one more formula which is quite useful to do and it is this formula.

(Refer Slide Time: 02:38)

Theorem: $\varphi(n) = n \prod_{p|n} (1 - 1/p)$. \prod = product.

Proof: Here p varies over the prime factors of n .

$$\text{Let } n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \text{ where } p_1 < p_2 < \cdots < p_k.$$

$$\text{Then } \varphi(n) = \varphi(p_1^{n_1}) \varphi(p_2^{n_2}) \cdots \varphi(p_k^{n_k}).$$

So, this formula is actually quite easy. It tells us that the Euler phi function is n into the product of $1 - 1/p$ where p varies over the prime factors of n . So, here p varies over the prime factors of n and this symbol that you see here, this stands for product. So, what we have seen here is that the Euler function can be computed the right-hand side here. So, let us go on about proving it. Suppose, we have n to be $p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, where we have let us say $p_1 < p_2, \dots, p_k$ just to say that we are looking at distinct primes here.

And then, as we have observed in the last slide, ϕ of n is going to be $\phi(p_1^{n_1}) \phi(p_2^{n_2}) \dots \phi(p_k^{n_k})$, this is using the second lemma that we have proved in the last lecture. So, here each of these ϕ values are known to us, we will simply put the ϕ values for each of these $p_i^{n_i}$ and then combine them to get the result for our n .

(Refer Slide Time: 04:37)

Theorem: $\phi(n) = n \prod_{p|n} (1 - 1/p)$.

Proof (contd.): Then $\phi(p_1^{n_1}) = \phi(p_2^{n_2}) = \dots = \phi(p_k^{n_k})$

$$\phi(n) = (p_1^{n_1} - p_1^{n_1-1}) (p_2^{n_2} - p_2^{n_2-1}) \dots (p_k^{n_k} - p_k^{n_k-1})$$

$$= \underline{p_1^{n_1}} \left(1 - \frac{1}{p_1}\right) \cdot \underline{p_2^{n_2}} \left(1 - \frac{1}{p_2}\right) \dots \underline{p_k^{n_k}} \left(1 - \frac{1}{p_k}\right)$$

$$= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \quad \square$$

So, then $\phi(n)$ is $p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} (1 - 1/p_1) (1 - 1/p_2) \dots (1 - 1/p_k)$. So, this is because we know that the ϕ value for $p_1^{n_1}$ is this, this is the $\phi(p_2^{n_2})$ and so on, where we get $\phi(p_k^{n_k})$ okay.

But now it is a simple thing to take the $p_1^{n_1}$ outside from here that will give us $1 - 1/p_1$ then we have $p_2^{n_2}$ and inside we have $1 - 1/p_2$, so on up to $p_k^{n_k}$, and we have $1 - 1/p_k$. And to combine all these together, we have that $p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} (1 - 1/p_1) (1 - 1/p_2) \dots (1 - 1/p_k)$ is going to give us $n \prod_{p|n} (1 - 1/p)$.

And then the remaining terms are simply product of 1 minus 1 upon p, where p divides n, that is all. It is a very simple proof, but it will help us in computing the phi functions for composite numbers or in general for any natural number n.

(Refer Slide Time: 06:37)

Examples:

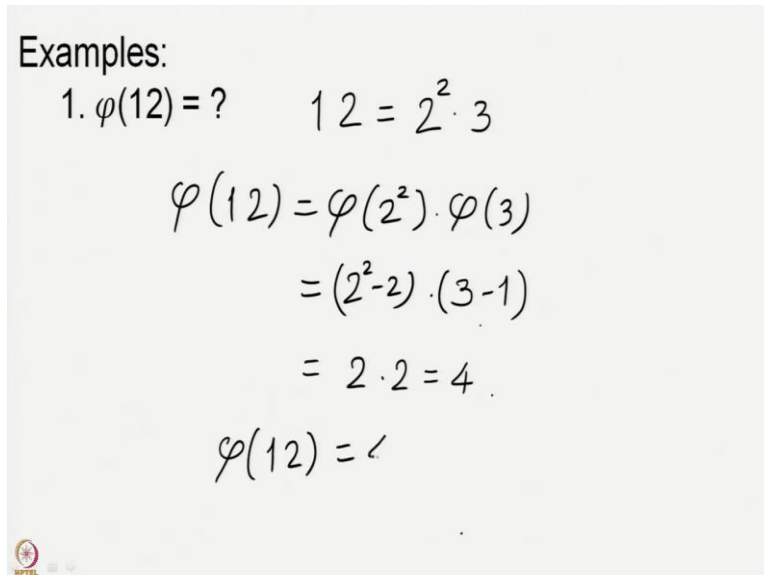
- $\varphi(12) = ?$ $12 = 2^2 \cdot 3$

$$\varphi(12) = \varphi(2^2) \cdot \varphi(3)$$

$$= (2^2 - 2) \cdot (3 - 1)$$

$$= 2 \cdot 2 = 4$$

$$\varphi(12) = 4$$



So, let us see whether we can apply this knowledge and compute the phi values. So, first of all, 12 can be written as 2 square into 3, 4 into 3 that is our 12. Therefore, phi of 12 is phi of 2 square into phi 3, 2 square is a prime power so this is going to be 2 square minus 2. This is going to be 3 minus 1 so we have 2 into 2, which gives us 4. So, phi 12 is equal to 4, quite a simple number.

(Refer Slide Time: 07:38)

Examples:

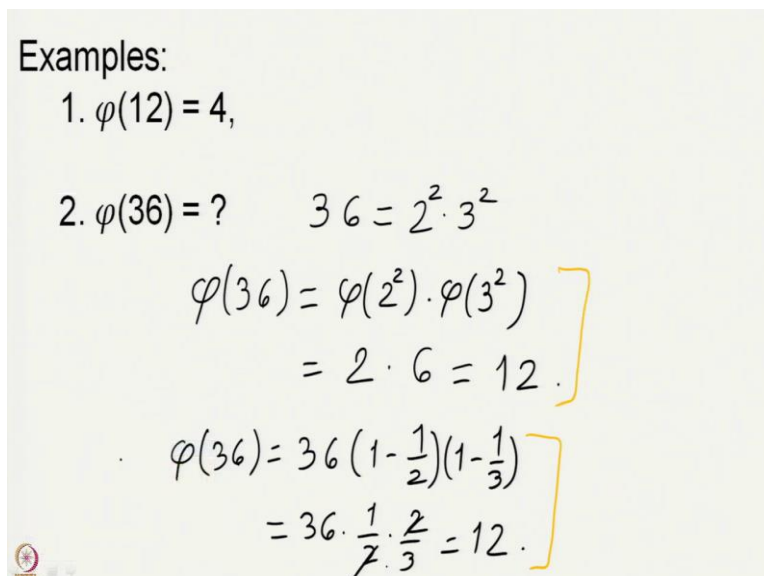
- $\varphi(12) = 4,$
- $\varphi(36) = ?$ $36 = 2^2 \cdot 3^2$

$$\varphi(36) = \varphi(2^2) \cdot \varphi(3^2)$$

$$= 2 \cdot 6 = 12$$

$$\varphi(36) = 36 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right)$$

$$= 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12$$



So, phi 12 is 4, what is the phi value at 36? So going by some of the examples that we have done in very first few lectures I am going to give you a minute to think about this and after your minute is up, we will start solving this problem. Alright so your minute is up, we have phi, Euler phi function of the number 36.

So, 36 is 6 square, so, this is 2 square into 3 square. And we should therefore compute the phi value for both 2 square and 3 square. So, phi 36 is phi 2 square and 2 phi 3 square, we have computed phi 2 square in our last slide, 2 square minus 2 so this is equal to 2, and 3 is phi of value 3 square will be 3 square minus 3 so that is 9 minus 3 which is 6, and so we get the Euler function on 36 to be equal to 12.

We can also use the formula that we developed in the last lemma. So, this will tell us that this should be 1 minus 1 by 2 1 minus 1 by 3, which is 36 into 1 by 2 into 2 by 3, which gives us 12. So, there are these 2 methods to compute the Euler phi function, the second method can be fed in a computer quite simply quite easily and the first one can be applied when you are doing the computation by hand. So, both these methods are quite useful. What we have obtained is 536 equal to 12 and I hope that you also got the same answer.

(Refer Slide Time 10:49)

Examples:

1. $\varphi(12) = 4$, prime factors of 60
2. $\varphi(36) = 12$, one 2, 3 and 5.
3. $\varphi(60) = ?$

$$\varphi(60) = 60 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right)$$

$$= \cancel{60}^4 \cdot \frac{1}{\cancel{2}} \cdot \frac{2}{\cancel{3}} \cdot \frac{4}{\cancel{5}} = 16.$$

$$\underline{\varphi(60) = 16.}$$

Let us do one more problem, the Euler five function on the number 60. So, I will give you 1 more minute to think about this problem and then we will see the solution, your minute starts now. Okay, your minute is up, we will apply the second method to solve this, which is to observe that the prime factors of 60 are, you have 2 dividing 60 and then 2 powers, 2 divides 60, actually. So, what you are left with is 15, so you have 3 and 5. And therefore phi of 60 is

60 into 1 minus 1 by 2, 1 minus 1 by 3, 1 minus 1 by 5. This is 60 into 1 by 2 into 2 by 3 into 4 by 5. So, this gets cancelled, 5 and 3 get cancelled for 60 to give you 4 so the answer is 16.

Let us see whether you also got the same answer. If you have any different answer, then perhaps it is time that you go back to your calculations and check where you may have possibly done a mistake. The Euler phi function is one very useful function, we are going to study this function later on while dealing with lots of other structures on the sets \mathbb{Z}_n . But to begin with, there is 1 very nice relation with the Euler phi function and the number n that we have. So, this is 1 very basic and very standard result, which we are going to state and prove.

(Refer Slide Time: 14:03)

Theorem: $\sum_{d|n} \phi(d) = n.$ $\sum = \text{sum}$
 d varies over divisors of n .

Proof:

Consider the set $\mathbb{Z}_n = \{1, 2, 3, \dots, n\}$

$\#\mathbb{Z}_n = n.$ For any $i \leq n, (i, n) | n.$

Let $A_d = \{0 < i \leq n : (i, n) = d\}.$ $A_{d_i} \cap A_{d_j} = \phi$ if $d_i \neq d_j$

\parallel disjoint union

Then $A_{d_1} \cup A_{d_2} \cup A_{d_3} \cup \dots \cup A_{d_k} = \mathbb{Z}_n.$
 d_i all divisors of n .

The result says that when you are taking summation of $\phi(d)$, where d varies over a divisors of a particular number n , then the answer you get is equal to n . So, here d varies over divisors of n and this sum is the symbol which denotes a sum. So, we are taking summation over $p \in D$ where d divides n and the answer is indeed equal to n . So, how does one prove this? The proof is quite nice. What we do is that consider the set \mathbb{Z}_n which is simply the set of natural numbers from 1, 2, 3 all the way up to n , and what we have is that the cardinality of \mathbb{Z}_n is n , this is something that we all agree with.

Further, for any i less than or equal to n , the GCD of i comma n has to be a factor of n . The GCD by very definition is that natural number which is greatest among the common divisors of i and n , so in particular it has to be a divisor of n . Therefore, suppose A_d denote the set of all the natural numbers up to n with the property that the GCD of i and n be equal to d , let A_d be this particular set. Then the union of A_1, A_d, A_1 is the first divisor of n , A_d, A_3 and so

on will give us our set Z_n . I may have used some symbols here which you may not have known about.

So, the symbol here which is given by the reverse sign of the product, this stands for disjoint union. This symbol says that we are first of all taking the union of the elements. But it also tells you that these sets are all disjoint and that is something which is not very difficult to check, because whenever you have elements coming from 2 different d_i , so A_{d_i} intersection A_{d_j} is going to be empty. This is because the elements of A_{d_i} have the property that they are GCD with your number n is d_i whereas A_{d_j} are the elements whose GCD with n is d_j . So, this is if d_i is different from d_j .

So, we have that this is a disjoint union and it gives you Z_n that is because every element in Z_n should have a GCD which divides n . So, on the left-hand side we have the d_i , all possible divisors of n and the union, the disjoint union of all these d_i gives us Z_n .

(Refer Slide Time: 18:18)

Theorem: $\sum_{d|n} \varphi(d) = n.$

Proof (contd.): Then

$$\sum_{d|n} \# A_d = \# Z_n = n.$$

To find $\# A_d$ for each $d|n$.

$$A_d = \{ 1 \leq i \leq n : (i, n) = d \}.$$

So, when you compute the cardinalities because the union is disjoint, what we get is that summation over d dividing n cardinality of these A_d is summation, cardinality of our set Z_n , which is n . So, we now need to find the cardinality of A_d for each divisor of n . So, let us see what is A_d once again. A_d is the set of all these elements with the property that i comma n is d , the GCD of i and n is d .


(Refer Slide Time: 19:19)

Theorem: $\sum_{d|n} \varphi(d) = n.$

Proof (contd.): Here $(i, n) = d$ if and only if

$$\left(\frac{i}{d}, \frac{n}{d}\right) = 1.$$

Thus $\# A_d = \left\{ 0 < i/d \leq n/d : (i/d, n/d) = 1 \right\}$



So, here GCD of i comma n is d if and only if GCD of i by d and n by d is 1. This is one very basic thing, which we have used quite a few times already. So, thus the cardinality of A_d is also equal to the cardinality of these elements with the property that these 2 numbers are co prime, but this is precisely your phi of n by d . So, each A_d has cardinality Euler phi function of the corresponding divisor of n . So, you have the divisor d and you get the Euler phi function of n by d .


(Refer Slide Time: 20:31)

Theorem: $\sum_{d|n} \varphi(d) = n.$

Proof (contd.): Then $\sum_{d|n} \# A_d = n$

$$= \sum_{d|n} \varphi(n/d) = n.$$

Therefore $\sum_{d|n} \varphi(d) = n.$ \square



And therefore, when we write this final thing down, then summation over d dividing n cardinality A_d , this is summation over d dividing n phi n by d and we have already seen this

to be equal to n , so this is n but once you are waiting over the divisors of n , the d and the set n by d 's are the same sets and therefore, we get that summation of $\phi(d)$, where d divides n is indeed equal to the set the number n . So, this is something which you can quite nicely check.

You know, often people say that mathematics is that particular branch where we do not have a laboratory where there are no experiments. But these kinds of results will not come unless you have experiments, people would have experimented on natural numbers, and then they would have thought about these results and only then they would have proved the results.

So, it is a different thing to have experiment. It is a different thing to have proofs, but both are very important components here. So, I invite you to take your favorite natural number n , take the n to be a composite number, take the n which has many prime factors say 3 or 4 so that you have many terms to look for and then check this thing for yourself that n is indeed summation $\phi(d)$ where d divides n .

You may also look at the numbers that we have looked up while completing the Euler ϕ functions, we computed $\phi(12)$ we completed $\phi(16)$ and we completed $\phi(36)$ those are nice numbers because there are many divisors. So, 36 in particular is 2 squares into 3 square so it will have many divisors.

So, these are the numbers for which you should try to do some experiments and get the feel of this thing otherwise doing the proofs only would be a bit of a dry thing. So, after having done this, what we now do is to go to higher study, but in our higher study we are going to be needing the concepts like groups and rings, when we go to study these numbers further.

So, we have various functions now, like the Euler ϕ function and so on, and we want to study the sets \mathbb{Z}_n further more deeply and so, we will need to use more structures on these sets. These structures happen to be the algebraic structures of groups and rings. So, it would be nice if you know these things already. What is a group?

(Refer Slide Time: 23:35)

• Groups: G together with a binary operation, $*$,

- Closure: $a * b \in G \quad \forall a, b \in G$
- Associativity: $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G.$
- Identity: $\exists 1 \in G$ such that $1 * a = a * 1 = a \quad \forall a \in G.$
- Inverse: $\forall a \in G \exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1.$

Group is basically a set to start with, it is a non empty set which comes equipped with a binary operation. So, binary operation means that there is a rule of starting with any 2 elements in the set in a particular order and you get one more element of the same set. This is what we mean by saying that there is a binary operation associated with the set.

So, a group is a non empty set, it can be finite, it can be infinite with the property that there is a binary operation defined on the set and this binary operation should satisfy some properties. So, the first property says that the set be closed under the binary operation, but this is same thing as saying that whenever you take 2 elements in the set, the applied value the binary operation when you apply to these 2 elements in that order, the further element that you get is also in the set this is what 1 means by saying that the set G be closed under this binary operation.

Second property says that there is associativity. For instance, if you are given n elements in the set and you want to compute the binary operation on all of them. How should you go? Meaning should you compute A_1, A_2 , then A_1, A_2 is third element in the group. So, you should be computing the A_1, A_2 with A_3 . And then you should look for A_1, A_2 with A_3 , this is yet another element and then you take the element A_4 or should you take A_1, A_2, A_3, A_4 and then take the binary operation. How should you go about doing this? So, associativity is the thing which tells you that this is all the same.

(Refer Slide Time: 25:37)

• Groups: G together with a binary operation, $*$,

- Closure: $a * b \in G \quad \forall a, b \in G$
- Associativity: $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G.$
- Identity: $\exists 1 \in G$ such that $1 * a = a * 1 = a \quad \forall a \in G.$
- Inverse: $\forall a \in G \exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1.$

So, this is a G , together with a binary operation, let us denote it by star. Then the first property says that the set be closed under this binary operation, which means that $a * b$ belongs to G , whenever you have a and b coming from G . Second property says that we have associativity, which says that the $a * b * c$ is equal to $a * (b * c)$ for every a, b, c in G .

This means that when you are applying the binary operation, then the order in which you apply this operation is not important if you have a, b, c, d you take $a * b * c * d$ and then take their star or you take $a * (b * c) * d$ and then take their star or you take $a * b * (c * d)$ and then take their star, all the elements that you are going to get are the same. So, which way you should bracket the elements is not important that is the Very important condition.

The another important condition is what is called the existence of identity element. This says that there is some element which we often denote by 1 in your say G such that $1 * a = a * 1 = a$ for every element in G . This says that there is one very distinguished element in your set G , which acts like the identity in multiplication which acts like the 1 when we take product or it acts like 0 when you take these sums.

So, this is the element such that taking star taking the binary operation with this element either in the first place or in the second place has no effect on any a so, there is this element. And finally, there is the action of existence of inverse, which says that for every a in G there exists an element which we denote by a^{-1} such that $a * a^{-1} = a^{-1} * a = 1$.

So, it tells you that for every a there is some another element, it could be equal to a or it could be an any different element such that the star of the binary operation of these 2 elements in any order gives you back the identity element. Now, there are these basic actions we will see some examples of the groups in the next lecture. But you should note first of all that the element 1 and the element a inverse for every a these are unique. These are some of the very basic statements that we often see in the theory of groups. So, I will not prove any of these results, I will assume that what is a group.

In the next lecture, I will start with some examples of groups and I will also talk about what we mean by a ring. But beyond giving you some very basic information, I will not be dealing with any other properties of these structures, but we will need to use them. So, it will be nice if you could go back and read some of the very basic books on groups and things. See you in the next lecture. Thank you.